AIDA64 Extreme

Navigation

Version	AIDA64 v6.25.5400
Benchmark Module	4.5.816.8-x64
Homepage	http://www.aida64.com/
Report Type	Quick Report [TRIAL VERSION]
Computer	VIETHOANG
Generator	bebos
Operating System	Microsoft Windows 10 Pro 10.0.19042.508
Date	2020-09-12
Time	21:11

Summary

Computer:

Computer Type	ACPI x64-based PC
Operating System	Microsoft Windows 10 Pro
OS Service Pack	[TRIAL VERSION]
Internet Explorer	11.508.19041.0
Edge	44.19041.423.0
DirectX	DirectX 12.0
Computer Name	VIETHOANG
User Name	bebos
Logon Domain	[TRIAL VERSION]
Date / Time	2020-09-12 / 21:11

Motherboard:

CPU Type	DualCore Intel Core i3-3220, 3300 MHz (33 x 100)
Motherboard Name	Unknown
Motherboard Chipset	Intel Panther Point B75, Intel Ivy Bridge
System Memory	[TRIAL VERSION]
DIMM3: Kingston 9905584-015.A00LF	[TRIAL VERSION]
BIOS Type	AMI (05/10/2013)
Communication Port	Communications Port (COM1)
Communication Port	Bluetooth SPP Driver (COM4)
Communication Port	Bluetooth SPP Driver (COM5)
Communication Port	Printer Port (LPT1)

Display:

Video Adapter	Intel(R) HD Graphics 2500 (2097650 KB)
Video Adapter	Intel(R) HD Graphics 2500 (2097650 KB)
Video Adapter	Intel(R) HD Graphics 2500 (2097650 KB)
3D Accelerator	Intel HD Graphics 2500
Monitor	Samsung SyncMaster E1920/E1920X/EX1920/EX1920X (Analog) [19" LCD] (HDBZ824304)

Multimedia:

Audio Adapter	Realtek ALC269 @ Intel Panther Point PCH - High Definition Audio Controller [C1]

Storage:

IDE Controller	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02

Navigation

Storage Controller	Microsoft Storage Spaces Controller
Disk Drive	P3-128 (119 GB)
Optical Drive	TSSTcorp CDDVDW SH-216DB (DVD+R9:8x, DVD-R9:8x, DVD+RW:16x/8x, DVD-RW:16x/6x, DVD-RAM:5x, DVD-ROM:16x, CD:48x/24x/48x DVD+RW/DVD-RW/DVD-RAM)
SMART Hard Disks Status	OK

Partitions:

C: (NTFS)	[TRIAL VERSION]
Total Size	[TRIAL VERSION]

Input:

Keyboard	HID Keyboard Device
Mouse	HID-compliant mouse

Network:

Primary IP Address	[TRIAL VERSION]
Primary MAC Address	F8-0F-41-B1-FA-FB
Network Adapter	Bluetooth Personal Area Network Device
Network Adapter	Realtek PCIe GbE Family Controller (192. [TRIAL VERSION])
Modem	SAMSUNG Mobile USB Modem

Peripherals:

Printer	Fax
Printer	Microsoft Print to PDF
Printer	Microsoft XPS Document Writer
Printer	OneNote for Windows 10
Printer	Send To OneNote 2016
USB2 Controller	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C1]
USB2 Controller	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C1]
USB3 Controller	Intel Panther Point PCH - USB 3.0 xHCI Controller [C1]
USB Device	CSR BlueCore Device
USB Device	Generic USB Hub
USB Device	Generic USB Hub
USB Device	SAMSUNG Android ADB Interface
USB Device	SAMSUNG Mobile USB Composite Device
USB Device	SAMSUNG Mobile USB Modem
USB Device	SMJ320H
USB Device	USB Composite Device
USB Device	USB Input Device
USB Device	USB Input Device
USB Device	USB Input Device

DMI:

DMI BIOS Vendor	FUJITSU // American Megatrends Inc.
DMI BIOS Version	4.09
DMI System Manufacturer	FUJITSU
DMI System Product	FMVD0400D
DMI System Version	
DMI System Serial Number	[TRIAL VERSION]
DMI System UUID	[TRIAL VERSION]
DMI Motherboard Manufacturer	FUJITSU
DMI Motherboard Product	JIB75Y3
DMI Motherboard Version	
DMI Motherboard Serial Number	[TRIAL VERSION]
DMI Chassis Manufacturer	FUJITSU
DMI Chassis Version	

DMI Chassis Serial Number	[TRIAL VERSION]
DMI Chassis Asset Tag	[TRIAL VERSION]
DMI Chassis Type	Desktop Case

Navigation

Computer Name

Type	Class	Computer Name
Computer Comment	Logical	
NetBIOS Name	Logical	VIETHOANG
DNS Host Name	Logical	VIETHOANG
DNS Domain Name	Logical	
Fully Qualified DNS Name	Logical	VIETHOANG
NetBIOS Name	Physical	VIETHOANG
DNS Host Name	Physical	VIETHOANG
DNS Domain Name	Physical	
Fully Qualified DNS Name	Physical	VIETHOANG

DMI

[BIOS]

BIOS Properties:

Vendor	FUJITSU // American Megatrends Inc.
Version	4.09
Release Date	05/10/2013
Size	3584 KB
System BIOS Version	4.9
Boot Devices	Floppy Disk, Hard Disk, CD-ROM
Capabilities	Flash BIOS, Shadow BIOS, Selectable Boot, EDD, BBS
Supported Standards	DMI, ACPI, PnP
Expansion Capabilities	PCI, USB
Virtual Machine	No

BIOS Manufacturer:

Company Name	American Megatrends Inc.
Product Information	https://ami.com/en/products/bios-uefi-firmware
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates

[System]

System Properties:

Manufacturer	FUJITSU
Product	FMVD0400D
Serial Number	[TRIAL VERSION]
Universal Unique ID	[TRIAL VERSION]
Universal Unique ID (GUID)	[TRIAL VERSION]
Wake-Up Type	Power Switch

[Motherboard]

Navigation

Motherboard Properties:

Manufacturer	FUJITSU
Product	JIB75Y3
Serial Number	[TRIAL VERSION]
Asset Tag	[TRIAL VERSION]
Asset Tag	[TRIAL VERSION]
Asset Tag	[TRIAL VERSION]

[Chassis]

Chassis Properties:

Manufacturer	FUJITSU
Serial Number	[TRIAL VERSION]
Asset Tag	[TRIAL VERSION]
Chassis Type	Desktop Case

[Processors / Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz]

Processor Properties:

Manufacturer	Intel(R) Corporation
Version	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
External Clock	100 MHz
Maximum Clock	3300 MHz
Current Clock	3300 MHz
Type	Central Processor
Voltage	1.5 V
Status	Enabled
Upgrade	Socket LGA1155
Socket Designation	LGA1155
HTT / CMP Units	2 / 2
Capabilities	64-bit

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	https://ark.intel.com/content/www/us/en/ark/search.html?q=Intel%20Core%20i3-3220
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Caches / Cache #1]

Cache Properties:

Type	Unified
Status	Enabled
Operational Mode	Write-Through
Associativity	8-way Set-Associative
Maximum Size	512 KB
Installed Size	512 KB
Error Correction	Single-bit ECC

[Caches / Cache #2]

Cache Properties:

Type	Unified
Status	Enabled

Operational Mode	Write-Through
Associativity	8-way Set-Associative
Maximum Size	128 KB
Installed Size	128 KB

Navigation

[Caches / Cache #3]

Cache Properties:

Type	Unified
Status	Enabled
Operational Mode	Write-Back
Associativity	12-way Set-Associative
Maximum Size	3 MB
Installed Size	3 MB
Error Correction	Single-bit ECC

[Memory Arrays / System Memory]

Memory Array Properties:

Location	Motherboard
Memory Array Function	System Memory
Error Correction	None
Max. Memory Capacity	32 GB
Memory Devices	4

[Memory Devices / DIMM1]

Memory Device Properties:

Form Factor	DIMM
Type	DDR3
Type Detail	Synchronous
Total Width	64-bit
Data Width	64-bit
Device Locator	DIMM1
Bank Locator	CHB-1

[Memory Devices / DIMM2]

Memory Device Properties:

Form Factor	DIMM
Type	DDR3
Type Detail	Synchronous
Size	4 GB
Max. Clock Speed	1600 MT/s
Current Clock Speed	1600 MT/s
Total Width	64-bit
Data Width	64-bit
Ranks	1
Device Locator	DIMM2
Bank Locator	CHB-0
Manufacturer	Kingston
Serial Number	8D10B9A5
Asset Tag	1450
Part Number	9905584-015.A00LF

Navigation

[Memory Devices / DIMM3]

Memory Device Properties:

Form Factor	DIMM
Type	DDR3
Type Detail	Synchronous
Total Width	64-bit
Data Width	64-bit
Device Locator	DIMM3
Bank Locator	CHA-1

[Memory Devices / DIMM4]

Memory Device Properties:

Form Factor	DIMM
Type	DDR3
Type Detail	Synchronous
Total Width	64-bit
Data Width	64-bit
Device Locator	DIMM4
Bank Locator	CHA-0

[System Slots / PCI1]

System Slot Properties:

Slot Designation	PCI1
Type	PCI
Usage	Available
Data Bus Width	32-bit
Length	Short
ID	1

[System Slots / PCI2]

System Slot Properties:

Slot Designation	PCI2
Type	PCI
Usage	Available
Data Bus Width	32-bit
Length	Short
ID	2

[Intel AMT]

Intel AMT Properties:

Intel AMT	Not Supported
IDE Redirection	Disabled
SOL	Disabled
AMT Network Interface	Disabled

[Intel vPro]

Navigation

Intel vPro Properties:

MEBX Version	8.0.0.69
ME Firmware Version	8.1.30.1350
PCH PCI Bus / Device / Function	0 / 31 / 0
PCH PCI Device ID	8086-1E49
Wired NIC PCI Bus / Device / Function	0 / 25 / 0
Wired NIC PCI Device ID	8086-FFFF
AMT	Not Supported
Anti-Theft	Not Supported
Anti-Theft PBA for Recovery	Not Supported
Anti-Theft WWAN	Not Supported
BIOS TXT	Supported
BIOS VT-d	Supported
BIOS VT-x	Supported
CPU VT-x	Supported, Enabled
CPU TXT	Not Supported
KVM	Not Supported
Local Wakeup Timer	Not Supported
Management Engine	Enabled
Small Business Advantage	Not Supported
Standard Manageability	Not Supported

Overclock

CPU Properties:

CPU Type	DualCore Intel Core i3-3220
CPU Alias	Ivy Bridge-DT
CPU Stepping	E1/L1/N0/P0
Engineering Sample	No
CPUID CPU Name	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
CPUID Revision	000306A9h
CPU VID	1.0107 V

CPU Speed:

CPU Clock	3292.9 MHz (original: [TRIAL VERSION] MHz)
CPU Multiplier	33x
CPU FSB	99.8 MHz (original: 100 MHz)
North Bridge Clock	3292.9 MHz
Memory Bus	798.3 MHz
DRAM:FSB Ratio	24:3

CPU Cache:

L1 Code Cache	32 KB per core
L1 Data Cache	[TRIAL VERSION]
L2 Cache	256 KB per core (On-Die, ECC, Full-Speed)
L3 Cache	3 MB (On-Die, ECC, Full-Speed)

Motherboard Properties:

Motherboard ID	63-0100-000001-00101111-122211-Chipset$JIB75Y3409_
Motherboard Name	Unknown

Chipset Properties:

Motherboard Chipset	Intel Panther Point B75, Intel Ivy Bridge

Navigation

Memory Timings	11-11-11-28 (CL-RCD-RP-RAS)
Command Rate (CR)	[TRIAL VERSION]
DIMM3: Kingston 9905584-015.A00LF	[TRIAL VERSION]

BIOS Properties:

System BIOS Date	05/10/2013
Video BIOS Date	02/13/12
DMI BIOS Version	4.09

Graphics Processor Properties:

Video Adapter	Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)
GPU Code Name	Ivy Bridge-DT GT1 (Integrated 8086 / 0152, Rev 09)
GPU Clock	349 MHz (original: [TRIAL VERSION] MHz)

Power Management

Power Management Properties:

Current Power Source	AC Line
Battery Status	No Battery
Full Battery Lifetime	Unknown
Remaining Battery Lifetime	Unknown

Portable Computer

Centrino (Carmel) Platform Compliancy:

CPU: Intel Pentium M (Banias/Dothan)	No (Intel Core i3-3220)
Chipset: Intel i855GM/PM	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel PRO/Wireless	No
System: Centrino Compliant	No

Centrino (Sonoma) Platform Compliancy:

CPU: Intel Pentium M (Dothan)	No (Intel Core i3-3220)
Chipset: Intel i915GM/PM	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel PRO/Wireless 2200/2915	No
System: Centrino Compliant	No

Centrino (Napa) Platform Compliancy:

CPU: Intel Core (Yonah) / Core 2 (Merom)	No (Intel Core i3-3220)
Chipset: Intel i945GM/PM	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel PRO/Wireless 3945/3965	No
System: Centrino Compliant	No

Centrino (Santa Rosa) Platform Compliancy:

CPU: Intel Core 2 (Merom/Penryn)	No (Intel Core i3-3220)
Chipset: Intel GM965/PM965	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel Wireless WiFi Link 4965	No
System: Centrino Compliant	No

Centrino 2 (Montevina) Platform Compliancy:

CPU: Intel Core 2 (Penryn)	No (Intel Core i3-3220)

Navigation

Chipset: Mobile Intel 4 Series	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel WiFi Link 5000 Series	No
System: Centrino 2 Compliant	No

Centrino (Calpella) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Arrandale/Clarksfield)	No (Intel Core i3-3220)
Chipset: Mobile Intel 5 Series	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Centrino (Huron River) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Sandy Bridge-MB)	No (Intel Core i3-3220)
Chipset: Mobile Intel 6 Series	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Centrino (Chief River) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Ivy Bridge-MB)	No (Intel Core i3-3220)
Chipset: Mobile Intel 7 Series	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Centrino (Shark Bay-MB) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Haswell-MB)	No (Intel Core i3-3220)
Chipset: Mobile Intel 8/9 Series	No (Intel Panther Point B75, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Sensor

Sensor Properties:

Sensor Type	ITE IT8728F (ISA 6B0h)
Chassis Intrusion Detected	Yes

Temperatures:

Motherboard	33 °C
CPU	37 °C
CPU Package	45 °C
CPU IA Cores	45 °C
CPU GT Cores	45 °C
CPU #1 / Core #1	44 °C
CPU #1 / Core #2	44 °C
PCH Diode	65 °C
Aux	40 °C
P3-128	[TRIAL VERSION]

Cooling Fans:

CPU	1232 RPM

Voltage Values:

CPU Core	2.220 V
CPU VID	0.841 V
+3.3 V	4.574 V

+5 V	7.140 V
+12 V	[TRIAL VERSION]

Navigation

Power Values:

CPU Package	3.28 W
CPU IA Cores	1.16 W
CPU GT Cores	[TRIAL VERSION]
CPU Uncore	2.12 W
Debug Info F	0224 FFFF FFFF 0000 0000
Debug Info T	40 33 37
Debug Info V	B9 B9 F3 EE E7 62 29 7D 88

CPU

CPU Properties:

CPU Type	DualCore Intel Core i3-3220, 3300 MHz (33 x 100)
CPU Alias	Ivy Bridge-DT
CPU Stepping	E1/L1/N0/P0
Instruction Set	x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, AVX
Original Clock	[TRIAL VERSION]
Min / Max CPU Multiplier	16x / 33x
Engineering Sample	No
L1 Code Cache	32 KB per core
L1 Data Cache	[TRIAL VERSION]
L2 Cache	256 KB per core (On-Die, ECC, Full-Speed)
L3 Cache	3 MB (On-Die, ECC, Full-Speed)

CPU Physical Info:

Package Type	1155 Contact FC-LGA
Package Size	37.5 mm x 37.5 mm
Process Technology	22 nm, CMOS, Cu, High-K + Metal Gate
Die Size	[TRIAL VERSION]
Typical Power	55 W

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	https://ark.intel.com/content/www/us/en/ark/search.html?q=Intel%20Core%20i3-3220
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Multi CPU:

Motherboard ID	JIB75Y3 FUJ
CPU #1	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
CPU #2	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
CPU #3	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
CPU #4	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz

CPU Utilization:

CPU #1 / Core #1 / SMT Unit #1	50%
CPU #1 / Core #1 / SMT Unit #2	0%
CPU #1 / Core #2 / SMT Unit #1	25%
CPU #1 / Core #2 / SMT Unit #2	0%

CPUID

Navigation

CPUID Properties:

CPUID Manufacturer	GenuineIntel
CPUID CPU Name	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
CPUID Revision	000306A9h
IA Brand ID	00h (Unknown)
Platform ID	4Ah / MC 02h (LGA1155)
Microcode Update Revision	21h
SMT / CMP Units	2 / 2
Tjmax Temperature	105 °C (221 °F)
CPU Thermal Design Power (TDP)	55 W
CPU IA Cores Thermal Design Current	112 A
CPU GT Cores Thermal Design Current	46 A
CPU Max Power Limit	Unlimited Power / 8.00 sec
CPU Power Limit 1 (Long Duration)	55 W / 1.00 sec (Locked)
CPU Power Limit 2 (Short Duration)	68.8 W / Unlimited Time (Locked)

Instruction Set:

64-bit x86 Extension (AMD64, Intel64)	Supported
AMD 3DNow!	Not Supported
AMD 3DNow! Professional	Not Supported
AMD 3DNowPrefetch	Not Supported
AMD Enhanced 3DNow!	Not Supported
AMD Extended MMX	Not Supported
AMD FMA4	Not Supported
AMD MisAligned SSE	Not Supported
AMD SSE4A	Not Supported
AMD XOP	Not Supported
Cyrix Extended MMX	Not Supported
Enhanced REP MOVSB/STOSB	Supported
Enqueue Stores	Not Supported
Galois Field New Instructions (GFNI)	Not Supported
Float-16 Conversion Instructions	Supported, Enabled
IA-64	Not Supported
IA AES Extensions	Not Supported
IA AVX	Supported, Enabled
IA AVX2	Not Supported
IA AVX-512 (AVX512F)	Not Supported
IA AVX-512 4x Fused Multiply-Add Single Precision (AVX512_4FMAPS)	Not Supported
IA AVX-512 4x Neural Network Instructions (AVX512_4VNNIW)	Not Supported
IA AVX-512 52-bit Integer Multiply-Add Instructions (AVX512_IFMA)	Not Supported
IA AVX-512 BF16 (AVX512_BF16)	Not Supported
IA AVX-512 Bit Algorithm (AVX512_BITALG)	Not Supported
IA AVX-512 Byte and Word Instructions (AVX512BW)	Not Supported
IA AVX-512 Conflict Detection Instructions (AVX512CD)	Not Supported
IA AVX-512 Doubleword and Quadword Instructions (AVX512DQ)	Not Supported
IA AVX-512 Exponential and Reciprocal Instructions (AVX512ER)	Not Supported
IA AVX-512 Intersection (AVX512_VP2INTERSECT)	Not Supported
IA AVX-512 Neural Network Instructions (AVX512_VNNI)	Not Supported
IA AVX-512 Prefetch Instructions (AVX512PF)	Not Supported
IA AVX-512 Vector Bit Manipulation Instructions (AVX512_VBMI)	Not Supported
IA AVX-512 Vector Bit Manipulation Instructions 2 (AVX512_VBMI2)	Not Supported
IA AVX-512 Vector Length Extensions (AVX512VL)	Not Supported

Navigation

IA AVX-512 VPOPCNTDQ	Not Supported
IA BMI1	Not Supported
IA BMI2	Not Supported
IA FMA	Not Supported
IA MMX	Supported
IA SHA Extensions	Not Supported
IA SSE	Supported
IA SSE2	Supported
IA SSE3	Supported
IA Supplemental SSE3	Supported
IA SSE4.1	Supported
IA SSE4.2	Supported
Vector AES (VAES)	Not Supported
VIA Alternate Instruction Set	Not Supported
ADCX / ADOX Instruction	Not Supported
CLDEMOTE Instruction	Not Supported
CLFLUSH Instruction	Supported
CLFLUSHOPT Instruction	Not Supported
CLWB Instruction	Not Supported
CLZERO Instruction	Not Supported
CMPXCHG8B Instruction	Supported
CMPXCHG16B Instruction	Supported
Conditional Move Instruction	Supported
Fast Short REP MOV Instruction	Not Supported
INVPCID Instruction	Not Supported
LAHF / SAHF Instruction	Supported
LZCNT Instruction	Not Supported
MCOMMIT Instruction	Not Supported
MONITOR / MWAIT Instruction	Supported
MONITORX / MWAITX Instruction	Not Supported
MOVBE Instruction	Not Supported
MOVDIR64B Instruction	Not Supported
MOVDIRI Instruction	Not Supported
PCLMULQDQ Instruction	Supported
PCOMMIT Instruction	Not Supported
PCONFIG Instruction	Not Supported
POPCNT Instruction	Supported
PREFETCHWT1 Instruction	Not Supported
PTWRITE Instruction	Not Supported
RDFSBASE / RDGSBASE / WRFSBASE / WRGSBASE Instruction	Supported
RDPRU Instruction	Not Supported
RDRAND Instruction	Not Supported
RDSEED Instruction	Not Supported
RDTSCP Instruction	Supported
SKINIT / STGI Instruction	Not Supported
SYSCALL / SYSRET Instruction	Not Supported
SYSENTER / SYSEXIT Instruction	Supported
Trailing Bit Manipulation Instructions	Not Supported
VIA FEMMS Instruction	Not Supported
VPCLMULQDQ Instruction	Not Supported
WBNOINVD Instruction	Not Supported

Security Features:

Advanced Cryptography Engine (ACE)	Not Supported
Advanced Cryptography Engine 2 (ACE2)	Not Supported

Navigation

Control-flow Enforcement Technology - Indirect Branch Tracking (CET_IBT)	Not Supported
Control-flow Enforcement Technology - Shadow Stack (CET_SS)	Not Supported
Data Execution Prevention (DEP, NX, EDB)	Supported
Enhanced Indirect Branch Restricted Speculation	Not Supported
Hardware Random Number Generator (RNG)	Not Supported
Hardware Random Number Generator 2 (RNG2)	Not Supported
Indirect Branch Predictor Barrier (IBPB)	Supported
Indirect Branch Restricted Speculation (IBRS)	Supported
L1D Flush	Supported
MD_CLEAR	Supported
Memory Protection Extensions (MPX)	Not Supported
PadLock Hash Engine (PHE)	Not Supported
PadLock Hash Engine 2 (PHE2)	Not Supported
PadLock Montgomery Multiplier (PMM)	Not Supported
PadLock Montgomery Multiplier 2 (PMM2)	Not Supported
Processor Serial Number (PSN)	Not Supported
Protection Keys for User-Mode Pages (PKU)	Not Supported
Read Processor ID (RDPID)	Not Supported
Safer Mode Extensions (SMX)	Not Supported
Secure Memory Encryption (SME)	Not Supported
SGX Launch Configuration (SGX_LC)	Not Supported
Software Guard Extensions (SGX)	Not Supported
Single Thread Indirect Branch Predictors (STIBP)	Supported
Speculative Store Bypass Disable (SSBD)	Supported
Supervisor Mode Access Prevention (SMAP)	Not Supported
Supervisor Mode Execution Protection (SMEP)	Supported
Total Memory Encryption (TME)	Not Supported
User-Mode Instruction Prevention (UMIP)	Not Supported

Power Management Features:

APM Power Reporting	Not Supported
Application Power Management (APM)	Not Supported
Automatic Clock Control	Supported
Configurable TDP (cTDP)	Not Supported
Connected Standby	Not Supported
Core C6 State (CC6)	Not Supported
Digital Thermometer	Supported
Dynamic FSB Frequency Switching	Not Supported
Enhanced Halt State (C1E)	Supported, Enabled
Enhanced SpeedStep Technology (EIST, ESS)	Supported, Enabled
Frequency ID Control	Not Supported
Hardware P-State Control	Not Supported
Hardware Thermal Control (HTC)	Not Supported
LongRun	Not Supported
LongRun Table Interface	Not Supported
Overstress	Not Supported
Package C6 State (PC6)	Not Supported
Parallax	Not Supported
PowerSaver 1.0	Not Supported
PowerSaver 2.0	Not Supported
PowerSaver 3.0	Not Supported
Processor Duty Cycle Control	Supported
Running Average Power Limit (RAPL)	Not Supported
Software Thermal Control	Not Supported
SpeedShift (SST, HWP)	Not Supported

Navigation

Temperature Sensing Diode	Not Supported
Thermal Monitor 1	Supported
Thermal Monitor 2	Supported
Thermal Monitor 3	Not Supported
Thermal Monitoring	Not Supported
Thermal Trip	Not Supported
Voltage ID Control	Not Supported

Virtualization Features:

AMD Virtual Interrupt Controller (AVIC)	Not Supported
Decode Assists	Not Supported
Encrypted Microcode Patch	Not Supported
Encrypted State (SEV-ES)	Not Supported
Extended Page Table (EPT)	Supported
Flush by ASID	Not Supported
Guest Mode Execute Trap Extension (GMET)	Not Supported
Hypervisor	Not Present
INVEPT Instruction	Supported
INVVPID Instruction	Supported
LBR Virtualization	Not Supported
Memory Bandwidth Enforcement (MBE)	Not Supported
Nested Paging (NPT, RVI)	Not Supported
NRIP Save (NRIPS)	Not Supported
PAUSE Filter Threshold	Not Supported
PAUSE Intercept Filter	Not Supported
Secure Encrypted Virtualization (SEV)	Not Supported
Secure Virtual Machine (SVM, Pacifica)	Not Supported
SVM Lock (SVML)	Not Supported
Virtual Transparent Encryption (VTE)	Not Supported
Virtualized GIF (vGIF)	Not Supported
Virtualized VMLOAD and VMSAVE	Not Supported
Virtual Machine Extensions (VMX, Vanderpool)	Supported
Virtual Processor ID (VPID)	Supported
VMCB Clean Bits	Not Supported

CPUID Features:

1 GB Page Size	Not Supported
36-bit Page Size Extension	Supported
5-Level Paging	Not Supported
64-bit DS Area	Supported
Adaptive Overclocking	Not Supported
Address Region Registers (ARR)	Not Supported
Code and Data Prioritization Technology (CDP)	Not Supported
Core Performance Boost (CPB)	Not Supported
Core Performance Counters	Not Supported
CPL Qualified Debug Store	Supported
Data Breakpoint Extension	Not Supported
Debug Trace Store	Supported
Debugging Extension	Supported
Deprecated FPU CS and FPU DS	Not Supported
Direct Cache Access	Not Supported
Dynamic Acceleration Technology (IDA)	Not Supported
Dynamic Configurable TDP (DcTDP)	Not Supported
Extended APIC Register Space	Not Supported
Fast Save & Restore	Supported

Navigation

Hardware Lock Elision (HLE)	Not Supported
Hybrid Boost	Not Supported
Hybrid CPU	Not Supported
Hyper-Threading Technology (HTT)	Supported, Enabled
Instruction Based Sampling	Not Supported
Invariant Time Stamp Counter	Supported
L1 Context ID	Not Supported
L2I Performance Counters	Not Supported
Lightweight Profiling	Not Supported
Local APIC On Chip	Supported
Machine Check Architecture (MCA)	Supported
Machine Check Exception (MCE)	Supported
Memory Configuration Registers (MCR)	Not Supported
Memory Type Range Registers (MTRR)	Supported
Model Specific Registers (MSR)	Supported
NB Performance Counters	Not Supported
Page Attribute Table (PAT)	Supported
Page Global Extension	Supported
Page Size Extension (PSE)	Supported
Pending Break Event (PBE)	Supported
Performance Time Stamp Counter (PTSC)	Not Supported
Physical Address Extension (PAE)	Supported
Platform Quality of Service Enforcement (PQE)	Not Supported
Platform Quality of Service Monitoring (PQM)	Not Supported
Process Context Identifiers (PCID)	Supported
Processor Feedback Interface	Not Supported
Processor Trace (PT)	Not Supported
Restricted Transactional Memory (RTM)	Not Supported
Self-Snoop	Supported
Time Stamp Counter (TSC)	Supported
Time Stamp Counter Adjust	Not Supported
Turbo Boost	Not Supported
Turbo Boost Max 3.0	Not Supported
Virtual Mode Extension	Supported
Watchdog Timer	Not Supported
x2APIC	Not Supported
XGETBV / XSETBV OS Enabled	Supported
XSAVE / XRSTOR / XSETBV / XGETBV Extended States	Supported
XSAVEOPT	Supported

CPUID Registers (CPU #0):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-00100800-3D9AE3BF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-02C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00001120
CPUID 00000006	00000075-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-9C000400
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603

Navigation

CPUID 0000000B	00000001-00000002-00000100-00000000 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000000 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-20202020-65746E49-2952286C [Intel(R)]
CPUID 80000003	726F4320-4D542865-33692029-3232332D [Core(TM) i3-322]
CPUID 80000004	50432030-20402055-30332E33-007A4847 [0 CPU @ 3.30GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

CPUID Registers (CPU #1 Virtual):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-01100800-3D9AE3BF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-02C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00001120
CPUID 00000006	00000075-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-9C000400
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000001 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000001 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-20202020-65746E49-2952286C [Intel(R)]
CPUID 80000003	726F4320-4D542865-33692029-3232332D [Core(TM) i3-322]
CPUID 80000004	50432030-20402055-30332E33-007A4847 [0 CPU @ 3.30GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

CPUID Registers (CPU #2):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-02100800-3D9AE3BF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]

Navigation

CPUID 00000004	1C03C163-02C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00001120
CPUID 00000006	00000075-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-9C000400
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000002 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000002 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-20202020-65746E49-2952286C [Intel(R)]
CPUID 80000003	726F4320-4D542865-33692029-3232332D [Core(TM) i3-322]
CPUID 80000004	50432030-20402055-30332E33-007A4847 [0 CPU @ 3.30GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

CPUID Registers (CPU #3 Virtual):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-03100800-3D9AE3BF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-02C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00001120
CPUID 00000006	00000075-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-9C000400
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000003 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000003 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-20202020-65746E49-2952286C [Intel(R)]
CPUID 80000003	726F4320-4D542865-33692029-3232332D [Core(TM) i3-322]
CPUID 80000004	50432030-20402055-30332E33-007A4847 [0 CPU @ 3.30GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

MSR Registers (CPU #0):

MSR 00000017	0004-0000-0000-0000 [PlatID = 1]
MSR 0000001B	0000-0000-FEE0-0900
MSR 00000035	0000-0000-0002-0004
MSR 00000048	0000-0000-0000-0000
MSR 00000049	< FAILED >
MSR 0000008B	0000-0021-0000-0000
MSR 000000CE	0008-1010-E001-2100 [eD = 0]
MSR 000000E7	0000-0172-4A5F-46DE [S200]
MSR 000000E7	0000-0172-5810-1A7C [S200]
MSR 000000E7	0000-0172-5D21-090A
MSR 000000E8	0000-013B-49E4-9D66 [S200]
MSR 000000E8	0000-013B-4BFD-EB76 [S200]
MSR 000000E8	0000-013B-4E40-AD6D
MSR 0000010B	< FAILED >
MSR 00000194	0000-0000-0011-0000
MSR 00000198	0000-1B38-0000-1000 [S200]
MSR 00000198	0000-1B38-0000-1000 [S200]
MSR 00000198	0000-1B38-0000-1000
MSR 00000199	0000-0000-0000-1000
MSR 0000019A	0000-0000-0000-0000
MSR 0000019B	0000-0000-0000-0010
MSR 0000019C	0000-0000-883F-0000 [S200]
MSR 0000019C	0000-0000-883E-0000 [S200]
MSR 0000019C	0000-0000-883D-0000
MSR 0000019D	0000-0000-0000-0000
MSR 000001A0	0000-0000-0085-0089
MSR 000001A2	0000-0000-0069-1400
MSR 000001A4	0000-0000-0000-0000
MSR 000001AA	0000-0000-0040-0000
MSR 000001AC	< FAILED >
MSR 000001AD	0000-0000-2121-2121
MSR 000001B0	0000-0000-0000-0006
MSR 000001B1	0000-0000-883C-0000
MSR 000001B2	0000-0000-0000-0000
MSR 000001FC	0000-0000-0014-005F
MSR 00000300	< FAILED >
MSR 0000030A	0000-0000-0000-0000 [S200]
MSR 0000030A	0000-0000-0000-0000 [S200]
MSR 0000030A	0000-0000-0000-0000
MSR 0000030B	0000-0000-0000-0000 [S200]
MSR 0000030B	0000-0000-0000-0000 [S200]
MSR 0000030B	0000-0000-0000-0000
MSR 00000480	00DA-0400-0000-0010
MSR 00000481	0000-007F-0000-0016
MSR 00000482	FFF9-FFFE-0401-E172
MSR 00000483	007F-FFFF-0003-6DFF
MSR 00000484	0000-FFFF-0000-11FF
MSR 00000485	0000-0000-1004-01E5
MSR 00000486	0000-0000-8000-0021
MSR 00000487	0000-0000-FFFF-FFFF
MSR 00000488	0000-0000-0000-2000
MSR 00000489	0000-0000-0017-27FF
MSR 0000048A	0000-0000-0000-002A
MSR 0000048B	0000-00FF-0000-0000
MSR 0000048C	0000-0F01-0611-4141

Navigation

Navigation

MSR 0000048D	0000-007F-0000-0016
MSR 0000048E	FFF9-FFFE-0400-6172
MSR 0000048F	007F-FFFF-0003-6DFB
MSR 00000490	0000-FFFF-0000-11FB
MSR 00000601	1814-1494-8000-0380
MSR 00000602	1814-1494-8000-0170
MSR 00000603	0000-0000-802C-2C2C
MSR 00000604	0000-0000-8068-6868
MSR 00000606	0000-0000-000A-1003
MSR 0000060A	0000-0000-0000-883B
MSR 0000060B	0000-0000-0000-8850
MSR 0000060C	0000-0000-0000-8857
MSR 0000060D	0000-0055-0A7E-7E01
MSR 00000610	8000-8226-0014-81B8
MSR 00000611	0000-0000-2B51-479C [S200]
MSR 00000611	0000-0000-2B52-2F5B [S200]
MSR 00000611	0000-0000-2B52-E075
MSR 00000613	< FAILED >
MSR 00000614	000D-0000-0160-01B8
MSR 00000618	< FAILED >
MSR 00000619	< FAILED >
MSR 0000061B	< FAILED >
MSR 0000061C	< FAILED >
MSR 00000638	0000-0000-0000-0000
MSR 00000639	0000-0000-1CE6-461F [S200]
MSR 00000639	0000-0000-1CE6-8F0D [S200]
MSR 00000639	0000-0000-1CE6-E655
MSR 0000063A	0000-0000-0000-0000
MSR 0000063B	< FAILED >
MSR 00000640	0000-0000-0000-0000
MSR 00000641	0000-0000-00D4-1D08 [S200]
MSR 00000641	0000-0000-00D4-1D08 [S200]
MSR 00000641	0000-0000-00D4-2B42
MSR 00000642	0000-0000-0000-0018
MSR 00000648	0000-0000-0000-0021
MSR 00000649	0160-0000-0000-0000
MSR 0000064A	0160-0000-0000-0000
MSR 0000064B	0000-0000-8000-0000
MSR 0000064C	0000-0000-0000-0000

MSR Registers (CPU #1):

MSR 00000017	0004-0000-0000-0000 [PlatID = 1]
MSR 0000001B	0000-0000-FEE0-0800
MSR 00000035	0000-0000-0002-0004
MSR 00000048	0000-0000-0000-0000
MSR 00000049	< FAILED >
MSR 0000008B	0000-0021-0000-0000
MSR 000000CE	0008-1010-E001-2100 [eD = 0]
MSR 000000E7	0000-011D-F34A-990A
MSR 000000E8	0000-0104-6002-6F15
MSR 0000010B	< FAILED >
MSR 00000194	0000-0000-0011-0000
MSR 00000198	0000-1AE6-0000-1000
MSR 00000199	0000-0000-0000-1000
MSR 0000019A	0000-0000-0000-0000

MSR 0000019B	0000-0000-0000-0010
MSR 0000019C	0000-0000-883C-0000
MSR 0000019D	0000-0000-0000-0000
MSR 000001A0	0000-0000-0085-0089
MSR 000001A2	0000-0000-0069-1400
MSR 000001A4	0000-0000-0000-0000
MSR 000001AA	0000-0000-0040-0000
MSR 000001AC	< FAILED >
MSR 000001AD	0000-0000-2121-2121
MSR 000001B0	0000-0000-0000-0006
MSR 000001B1	0000-0000-883B-0000
MSR 000001B2	0000-0000-0000-0000
MSR 000001FC	0000-0000-0014-005F
MSR 00000300	< FAILED >
MSR 0000030A	0000-0000-0000-0000
MSR 0000030B	0000-0000-0000-0000
MSR 00000480	00DA-0400-0000-0010
MSR 00000481	0000-007F-0000-0016
MSR 00000482	FFF9-FFFE-0401-E172
MSR 00000483	007F-FFFF-0003-6DFF
MSR 00000484	0000-FFFF-0000-11FF
MSR 00000485	0000-0000-1004-01E5
MSR 00000486	0000-0000-8000-0021
MSR 00000487	0000-0000-FFFF-FFFF
MSR 00000488	0000-0000-0000-2000
MSR 00000489	0000-0000-0017-27FF
MSR 0000048A	0000-0000-0000-002A
MSR 0000048B	0000-00FF-0000-0000
MSR 0000048C	0000-0F01-0611-4141
MSR 0000048D	0000-007F-0000-0016
MSR 0000048E	FFF9-FFFE-0400-6172
MSR 0000048F	007F-FFFF-0003-6DFB
MSR 00000490	0000-FFFF-0000-11FB
MSR 00000601	1814-1494-8000-0380
MSR 00000602	1814-1494-8000-0170
MSR 00000603	0000-0000-802C-2C2C
MSR 00000604	0000-0000-8068-6868
MSR 00000606	0000-0000-000A-1003
MSR 0000060A	0000-0000-0000-883B
MSR 0000060B	0000-0000-0000-8850
MSR 0000060C	0000-0000-0000-8857
MSR 0000060D	0000-0055-25F0-4732
MSR 00000610	8000-8226-0014-81B8
MSR 00000611	0000-0000-2B55-FE3D
MSR 00000613	< FAILED >
MSR 00000614	000D-0000-0160-01B8
MSR 00000618	< FAILED >
MSR 00000619	< FAILED >
MSR 0000061B	< FAILED >
MSR 0000061C	< FAILED >
MSR 00000638	0000-0000-0000-0000
MSR 00000639	0000-0000-1CE7-6EA8
MSR 0000063A	0000-0000-0000-0000
MSR 0000063B	< FAILED >
MSR 00000640	0000-0000-0000-0000

Navigation

MSR 00000641	0000-0000-00D4-2B42
MSR 00000642	0000-0000-0000-0018
MSR 00000648	0000-0000-0000-0021
MSR 00000649	0160-0000-0000-0000
MSR 0000064A	0160-0000-0000-0000
MSR 0000064B	0000-0000-8000-0000
MSR 0000064C	0000-0000-0000-0000

MSR Registers (CPU #2):

MSR 00000017	0004-0000-0000-0000 [PlatID = 1]
MSR 0000001B	0000-0000-FEE0-0800
MSR 00000035	0000-0000-0002-0004
MSR 00000048	0000-0000-0000-0000
MSR 00000049	< FAILED >
MSR 0000008B	0000-0021-0000-0000
MSR 000000CE	0008-1010-E001-2100 [eD = 0]
MSR 000000E7	0000-013B-5393-6A23
MSR 000000E8	0000-011C-3D0C-35CD
MSR 0000010B	< FAILED >
MSR 00000194	0000-0000-0011-0000
MSR 00000198	0000-1AE6-0000-1000
MSR 00000199	0000-0000-0000-1000
MSR 0000019A	0000-0000-0000-0000
MSR 0000019B	0000-0000-0000-0010
MSR 0000019C	0000-0000-883C-0000
MSR 0000019D	0000-0000-0000-0000
MSR 000001A0	0000-0000-0085-0089
MSR 000001A2	0000-0000-0069-1400
MSR 000001A4	0000-0000-0000-0000
MSR 000001AA	0000-0000-0040-0000
MSR 000001AC	< FAILED >
MSR 000001AD	0000-0000-2121-2121
MSR 000001B0	0000-0000-0000-0006
MSR 000001B1	0000-0000-883B-0000
MSR 000001B2	0000-0000-0000-0000
MSR 000001FC	0000-0000-0014-005F
MSR 00000300	< FAILED >
MSR 0000030A	0000-0000-0000-0000
MSR 0000030B	0000-0000-0000-0000
MSR 00000480	00DA-0400-0000-0010
MSR 00000481	0000-007F-0000-0016
MSR 00000482	FFF9-FFFE-0401-E172
MSR 00000483	007F-FFFF-0003-6DFF
MSR 00000484	0000-FFFF-0000-11FF
MSR 00000485	0000-0000-1004-01E5
MSR 00000486	0000-0000-8000-0021
MSR 00000487	0000-0000-FFFF-FFFF
MSR 00000488	0000-0000-0000-2000
MSR 00000489	0000-0000-0017-27FF
MSR 0000048A	0000-0000-0000-002A
MSR 0000048B	0000-00FF-0000-0000
MSR 0000048C	0000-0F01-0611-4141
MSR 0000048D	0000-007F-0000-0016
MSR 0000048E	FFF9-FFFE-0400-6172
MSR 0000048F	007F-FFFF-0003-6DFB

Navigation

MSR 00000490	0000-FFFF-0000-11FB
MSR 00000601	1814-1494-8000-0380
MSR 00000602	1814-1494-8000-0170
MSR 00000603	0000-0000-802C-2C2C
MSR 00000604	0000-0000-8068-6868
MSR 00000606	0000-0000-000A-1003
MSR 0000060A	0000-0000-0000-883B
MSR 0000060B	0000-0000-0000-8850
MSR 0000060C	0000-0000-0000-8857
MSR 0000060D	0000-0055-25F0-4732
MSR 00000610	8000-8226-0014-81B8
MSR 00000611	0000-0000-2B55-FE3D
MSR 00000613	< FAILED >
MSR 00000614	000D-0000-0160-01B8
MSR 00000618	< FAILED >
MSR 00000619	< FAILED >
MSR 0000061B	< FAILED >
MSR 0000061C	< FAILED >
MSR 00000638	0000-0000-0000-0000
MSR 00000639	0000-0000-1CE7-6EA8
MSR 0000063A	0000-0000-0000-0000
MSR 0000063B	< FAILED >
MSR 00000640	0000-0000-0000-0000
MSR 00000641	0000-0000-00D4-2B42
MSR 00000642	0000-0000-0000-0018
MSR 00000648	0000-0000-0000-0021
MSR 00000649	0160-0000-0000-0000
MSR 0000064A	0160-0000-0000-0000
MSR 0000064B	0000-0000-8000-0000
MSR 0000064C	0000-0000-0000-0000

MSR Registers (CPU #3):

MSR 00000017	0004-0000-0000-0000 [PlatID = 1]
MSR 0000001B	0000-0000-FEE0-0800
MSR 00000035	0000-0000-0002-0004
MSR 00000048	0000-0000-0000-0000
MSR 00000049	< FAILED >
MSR 0000008B	0000-0021-0000-0000
MSR 000000CE	0008-1010-E001-2100 [eD = 0]
MSR 000000E7	0000-0125-B870-9766
MSR 000000E8	0000-010A-64AE-955B
MSR 0000010B	< FAILED >
MSR 00000194	0000-0000-0011-0000
MSR 00000198	0000-1AE6-0000-1000
MSR 00000199	0000-0000-0000-1000
MSR 0000019A	0000-0000-0000-0000
MSR 0000019B	0000-0000-0000-0010
MSR 0000019C	0000-0000-883F-0000
MSR 0000019D	0000-0000-0000-0000
MSR 000001A0	0000-0000-0085-0089
MSR 000001A2	0000-0000-0069-1400
MSR 000001A4	0000-0000-0000-0000
MSR 000001AA	0000-0000-0040-0000
MSR 000001AC	< FAILED >
MSR 000001AD	0000-0000-2121-2121

MSR 000001B0	0000-0000-0000-0006
MSR 000001B1	0000-0000-883B-0000
MSR 000001B2	0000-0000-0000-0000
MSR 000001FC	0000-0000-0014-005F
MSR 00000300	< FAILED >
MSR 0000030A	0000-0000-0000-0000
MSR 0000030B	0000-0000-0000-0000
MSR 00000480	00DA-0400-0000-0010
MSR 00000481	0000-007F-0000-0016
MSR 00000482	FFF9-FFFE-0401-E172
MSR 00000483	007F-FFFF-0003-6DFF
MSR 00000484	0000-FFFF-0000-11FF
MSR 00000485	0000-0000-1004-01E5
MSR 00000486	0000-0000-8000-0021
MSR 00000487	0000-0000-FFFF-FFFF
MSR 00000488	0000-0000-0000-2000
MSR 00000489	0000-0000-0017-27FF
MSR 0000048A	0000-0000-0000-002A
MSR 0000048B	0000-00FF-0000-0000
MSR 0000048C	0000-0F01-0611-4141
MSR 0000048D	0000-007F-0000-0016
MSR 0000048E	FFF9-FFFE-0400-6172
MSR 0000048F	007F-FFFF-0003-6DFB
MSR 00000490	0000-FFFF-0000-11FB
MSR 00000601	1814-1494-8000-0380
MSR 00000602	1814-1494-8000-0170
MSR 00000603	0000-0000-802C-2C2C
MSR 00000604	0000-0000-8068-6868
MSR 00000606	0000-0000-000A-1003
MSR 0000060A	0000-0000-0000-883B
MSR 0000060B	0000-0000-0000-8850
MSR 0000060C	0000-0000-0000-8857
MSR 0000060D	0000-0055-25F0-4732
MSR 00000610	8000-8226-0014-81B8
MSR 00000611	0000-0000-2B55-FF95
MSR 00000613	< FAILED >
MSR 00000614	000D-0000-0160-01B8
MSR 00000618	< FAILED >
MSR 00000619	< FAILED >
MSR 0000061B	< FAILED >
MSR 0000061C	< FAILED >
MSR 00000638	0000-0000-0000-0000
MSR 00000639	0000-0000-1CE7-6F6D
MSR 0000063A	0000-0000-0000-0000
MSR 0000063B	< FAILED >
MSR 00000640	0000-0000-0000-0000
MSR 00000641	0000-0000-00D4-2B42
MSR 00000642	0000-0000-0000-0018
MSR 00000648	0000-0000-0000-0021
MSR 00000649	0160-0000-0000-0000
MSR 0000064A	0160-0000-0000-0000
MSR 0000064B	0000-0000-8000-0000
MSR 0000064C	0000-0000-0000-0000

Navigation

Motherboard

Navigation

Motherboard Properties:

Motherboard ID	63-0100-000001-00101111-122211-Chipset$JIB75Y3409_
Motherboard Name	Unknown

Front Side Bus Properties:

Bus Type	BCLK
Real Clock	100 MHz
Effective Clock	100 MHz

Memory Bus Properties:

Bus Type	DDR3 SDRAM
Bus Width	64-bit
DRAM:FSB Ratio	24:3
Real Clock	800 MHz (DDR)
Effective Clock	1600 MHz
Bandwidth	[TRIAL VERSION] MB/s

Chipset Bus Properties:

Bus Type	Intel Direct Media Interface v2.0

Memory

Physical Memory:

Total	[TRIAL VERSION]
Used	[TRIAL VERSION]
Free	638 MB
Utilization	[TRIAL VERSION]

Virtual Memory:

Total	5377 MB
Used	3895 MB
Free	1482 MB
Utilization	72 %

Paging File:

Paging File	C:\pagefile.sys
Current Size	1408 MB
Current / Peak Usage	216 MB / 513 MB
Utilization	15 %

Physical Address Extension (PAE):

Supported by Operating System	Yes
Supported by CPU	Yes
Active	Yes

SPD

Navigation

[DIMM3: [TRIAL VERSION]]

Memory Module Properties:

Module Name	[TRIAL VERSION]
Serial Number	8D10B9A5h (2780369037)
Manufacture Date	Week 50 / 2014
Module Size	4 GB (1 rank, 8 banks)
Module Type	[TRIAL VERSION]
Memory Type	DDR3 SDRAM
Memory Speed	DDR3-1600 (800 MHz)
Module Width	64 bit
Module Voltage	1.5 V
Error Detection Method	None
Refresh Rate	Normal (7.8 us)

Memory Timings:

@ 800 MHz	11-11-11-28 (CL-RCD-RP-RAS) / 39-208-5-12-6-6-24 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 761 MHz	10-10-10-27 (CL-RCD-RP-RAS) / 37-199-5-12-6-6-23 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 685 MHz	9-9-9-24 (CL-RCD-RP-RAS) / 33-179-5-11-6-6-21 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 609 MHz	8-8-8-22 (CL-RCD-RP-RAS) / 30-159-4-10-5-5-19 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 533 MHz	7-7-7-19 (CL-RCD-RP-RAS) / 26-139-4-8-4-4-16 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 457 MHz	6-6-6-16 (CL-RCD-RP-RAS) / 22-119-3-7-4-4-14 (RC-RFC-RRD-WR-WTR-RTP-FAW)

Memory Module Features:

Auto Self Refresh (ASR)	Supported
DLL-Off Mode	Supported
Extended Temperature Range	Supported
Extended Temperature 1X Refresh Rate	Not Supported
Module Thermal Sensor	Not Supported
On-Die Thermal Sensor Readout (ODTS)	Not Supported
Partial Array Self Refresh (PASR)	Not Supported
RZQ/6	Supported
RZQ/7	Supported

Memory Module Manufacturer:

Company Name	Kingston Technology Corporation
Product Information	https://www.kingston.com/en/memory

Chipset

[North Bridge: Intel Ivy Bridge-DT IMC]

North Bridge Properties:

North Bridge	Intel Ivy Bridge-DT IMC
Supported Memory Types	DDR3-1066, DDR3-1333, DDR3-1600 SDRAM
Maximum Memory Amount	32 GB
Revision	09
Process Technology	22 nm
VT-d	Not Supported
Extended APIC (x2APIC)	Not Supported

Navigation

Memory Controller:

Type	Dual Channel (128-bit)
Active Mode	Single Channel (64-bit)

Memory Timings:

CAS Latency (CL)	11T
RAS To CAS Delay (tRCD)	11T
RAS Precharge (tRP)	11T
RAS Active Time (tRAS)	28T
Row Refresh Cycle Time (tRFC)	208T
Command Rate (CR)	1T
RAS To RAS Delay (tRRD)	5T
Write Recovery Time (tWR)	12T
Read To Read Delay (tRTR)	Same Rank: 4T, Different Rank: 1T, Different DIMM: 3T
Read To Write Delay (tRTW)	Same Rank: 3T, Different Rank: 5T, Different DIMM: 5T
Write To Read Delay (tWTR)	6T, Different Rank: 1T, Different DIMM: 1T
Write To Write Delay (tWTW)	Same Rank: 4T, Different Rank: 3T, Different DIMM: 5T
Read To Precharge Delay (tRTP)	6T
Four Activate Window Delay (tFAW)	24T
Write CAS Latency (tWCL)	8T
CKE Min. Pulse Width (tCKE)	4T
Refresh Period (tREF)	6240T
Round Trip Latency (tRTL)	DIMM4: 32T
I/O Latency (tIOL)	DIMM4: 0T
Burst Length (BL)	8

Error Correction:

ECC	Not Supported
ChipKill ECC	Not Supported
RAID	Not Supported
ECC Scrubbing	Not Supported

Memory Slots:

DRAM Slot #1	4 GB (DDR3 SDRAM)

Integrated Graphics Controller:

Graphics Controller Type	Intel HD Graphics 2500
Graphics Controller Status	Enabled
Graphics Frame Buffer Size	64 MB

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[South Bridge: [TRIAL VERSION]]

South Bridge Properties:

South Bridge	[TRIAL VERSION]
Revision / Stepping	04 / C1
Package Type	942 Ball FC-BGA
Package Size	27 mm x 27 mm
Process Technology	65 nm

Die Size	[TRIAL VERSION] mm2
Core Voltage	1.05 V
TDP	6.7 W

Navigation

High Definition Audio:

Codec Name	Realtek ALC269
Codec ID	10EC0269h / 10CF9000h
Codec Revision	1001h
Codec Type	Audio

PCI Express Controller:

PCI-E 2.0 x1 port #1	Empty
PCI-E 2.0 x1 port #2	In Use @ x1 (Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter)

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

BIOS

BIOS Properties:

BIOS Type	AMI UEFI
BIOS Version	4.09
SMBIOS Version	2.6
UEFI Boot	Yes
Secure Boot	Not Supported
System BIOS Date	05/10/2013
Video BIOS Date	02/13/12

BIOS Manufacturer:

Company Name	American Megatrends Inc.
Product Information	https://ami.com/en/products/bios-uefi-firmware
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates

ACPI

[APIC: Multiple APIC Description Table]

ACPI Table Properties:

ACPI Signature	APIC
Table Description	Multiple APIC Description Table
Memory Address	D993A4F8h
Table Length	114 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	AMI

Creator Revision	00010013h
Local APIC Address	FEE00000h

Navigation

Processor Local APIC:

ACPI Processor ID	01h
APIC ID	00h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	02h
APIC ID	02h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	03h
APIC ID	01h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	04h
APIC ID	03h
Status	Enabled

I/O APIC:

I/O APIC ID	02h
I/O APIC Address	FEC00000h
Global System Interrupt Base	00000000h

Interrupt Source Override:

Bus	ISA
Source	IRQ0
Global System Interrupt	00000002h
Polarity	Conforms to the specifications of the bus
Trigger Mode	Conforms to the specifications of the bus

Interrupt Source Override:

Bus	ISA
Source	IRQ9
Global System Interrupt	00000009h
Polarity	Active High
Trigger Mode	Level-Triggered

Local APIC NMI:

ACPI Processor ID	FFh
Local ACPI LINT#	01h
Polarity	Active High
Trigger Mode	Edge-Triggered

[ASF!: Alert Standard Format Table]

ACPI Table Properties:

ACPI Signature	ASF!
Table Description	Alert Standard Format Table
Memory Address	D993C070h
Table Length	121 bytes

Navigation

OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	TFSM
Creator Revision	000F4240h

ASF_INFO:

Min Watchdog Reset Value	60 sec
Min ASF Sensor Interpoll Wait Time	25 msec
System ID	207Ah
IANA Manufacturer ID	00-00-00-D3h

ASF_RCTL:

Numer of Controls	4
Array Element Length	4

ASF_RMCP:

Remote Control Capabilities	20-18-00-00-00-12-F0h
RMCP Boot Options Completion Code	01h (No options to process)
RMCP IANA Enterprise ID	00-00-00-00h
RMCP Special Command	00h
RMCP Special Command Parameter	0000h
RMCP Boot Options	0000h
RMCP OEM Parameters	0000h

[BOOT: Simple Boot Flag Table]

ACPI Table Properties:

ACPI Signature	BOOT
Table Description	Simple Boot Flag Table
Memory Address	D993A650h
Table Length	40 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h

[DSDT: Differentiated System Description Table]

ACPI Table Properties:

ACPI Signature	DSDT
Table Description	Differentiated System Description Table
Memory Address	D99301A0h
Table Length	41537 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	INTL
Creator Revision	20051117h

nVIDIA SLI:

SLI Certification	Not Present
PCI 0-0-0-0 (Direct I/O)	8086-0150 (Intel)
PCI 0-0-0-0 (HAL)	8086-0150 (Intel)

Navigation

Lucid Virtu:

Virtu Certification	Not Present

[FACP: Fixed ACPI Description Table]

ACPI Table Properties:

ACPI Signature	FACP
Table Description	Fixed ACPI Description Table
Memory Address	D9930118h
Table Length	132 bytes
OEM ID	FUJ
OEM Table ID	PC
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h
FACS Address	D9EB4040h
DSDT Address	D99301A0h
SMI Command Port	000000B2h
PM Timer	00000408h

[FACP: Fixed ACPI Description Table]

ACPI Table Properties:

ACPI Signature	FACP
Table Description	Fixed ACPI Description Table
Memory Address	00000000-D993A3E8h
Table Length	268 bytes
OEM ID	FUJ
OEM Table ID	PC
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h
FACS Address	D9EB4080h / 00000000-00000000h
DSDT Address	D99301A0h / 00000000-D99301A0h
SMI Command Port	000000B2h
PM Timer	00000408h

[FACS: Firmware ACPI Control Structure]

ACPI Table Properties:

ACPI Signature	FACS
Table Description	Firmware ACPI Control Structure
Memory Address	D9EB4040h
Table Length	64 bytes
Hardware Signature	00000000h
Waking Vector	00000000h
Global Lock	00000000h

[FBPT: Firmware Basic Boot Performance Table]

ACPI Table Properties:

ACPI Signature	FBPT
Table Description	Firmware Basic Boot Performance Table

Memory Address	00000000-DA2FB038h
Table Length	56 bytes

Navigation

[FPDT: Firmware Performance Data Table]

ACPI Table Properties:

ACPI Signature	FPDT
Table Description	Firmware Performance Data Table
Memory Address	D993A570h
Table Length	68 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h
FBPT Address	00000000-DA2FB038h
S3PT Address	00000000-DA2FB018h

[HPET: IA-PC High Precision Event Timer Table]

ACPI Table Properties:

ACPI Signature	HPET
Table Description	IA-PC High Precision Event Timer Table
Memory Address	D993A678h
Table Length	56 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	AMI.
Creator Revision	00000005h
HPET Address	00000000-FED00000h
Vendor ID	8086h
Revision	01h
Number of Timers	8
Counter Size	64-bit
Minimum Clock Ticks	14318
Page Protection	No Guarantee
OEM Attribute	0h
LegacyReplacement IRQ Routing	Supported

[MCFG: Memory Mapped Configuration Space Base Address Description Table]

ACPI Table Properties:

ACPI Signature	MCFG
Table Description	Memory Mapped Configuration Space Base Address Description Table
Memory Address	D993A5B8h
Table Length	60 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	MSFT
Creator Revision	00000097h
Config Space Address	00000000-F8000000h
PCI Segment	0000h

Start Bus Number	00h
End Bus Number	3Fh

Navigation

[MSDM: Microsoft Data Management Table]

ACPI Table Properties:

ACPI Signature	MSDM
Table Description	Microsoft Data Management Table
Memory Address	D993A5F8h
Table Length	85 bytes
OEM ID	FUJ
OEM Table ID	PC
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h
SLS Version	1
SLS Data Type	1
SLS Data Length	29
SLS Data	WJND6-YR6F8-629WF-9GQDC-TMQH2

[RSD PTR: Root System Description Pointer]

ACPI Table Properties:

ACPI Signature	RSD PTR
Table Description	Root System Description Pointer
Memory Address	000F05C0h
Table Length	36 bytes
OEM ID	FUJ
RSDP Revision	2 (ACPI 2.0+)
RSDT Address	D9930028h
XSDT Address	00000000-D9930080h

[RSDT: Root System Description Table]

ACPI Table Properties:

ACPI Signature	RSDT
Table Description	Root System Description Table
Memory Address	D9930028h
Table Length	84 bytes
OEM ID	FUJ
OEM Table ID	PC
OEM Revision	40900000h
Creator ID	MSFT
Creator Revision	00010013h
RSDT Entry #0	D9930118h (FACP)
RSDT Entry #1	D993A4F8h (APIC)
RSDT Entry #2	D993A570h (FPDT)
RSDT Entry #3	D993A5B8h (MCFG)
RSDT Entry #4	D993A5F8h (MSDM)
RSDT Entry #5	D993A650h (BOOT)
RSDT Entry #6	D993A678h (HPET)
RSDT Entry #7	D993A6B0h (SSDT)
RSDT Entry #8	D993AA20h (SLIC)
RSDT Entry #9	D993AB98h (SSDT)

RSDT Entry #10	D993B548h (SSDT)
RSDT Entry #11	D993C070h (ASF!)

Navigation

[S3PT: S3 Performance Table]

ACPI Table Properties:

ACPI Signature	S3PT
Table Description	S3 Performance Table
Memory Address	00000000-DA2FB018h
Table Length	32 bytes

[SLIC: Software Licensing Description Table]

ACPI Table Properties:

ACPI Signature	SLIC
Table Description	Software Licensing Description Table
Memory Address	D993AA20h
Table Length	374 bytes
OEM ID	FUJ
OEM Table ID	PC
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h
SLIC Version	v2.1

OEM Public Key:

Key Type	06h
Version	02h
Algorithm	00002400h
Magic	RSA1
Bit Length	1024
Exponent	65537

SLIC Marker:

Version	00020001h
OEM ID	FUJ
OEM Table ID	PC
Windows Flag	WINDOWS

[SSDT: Secondary System Description Table]

ACPI Table Properties:

ACPI Signature	SSDT
Table Description	Secondary System Description Table
Memory Address	D993A6B0h
Table Length	877 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	INTL
Creator Revision	20091112h

[SSDT: Secondary System Description Table]

Navigation

ACPI Table Properties:

ACPI Signature	SSDT
Table Description	Secondary System Description Table
Memory Address	D993AB98h
Table Length	2474 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	INTL
Creator Revision	20051117h

[SSDT: Secondary System Description Table]

ACPI Table Properties:

ACPI Signature	SSDT
Table Description	Secondary System Description Table
Memory Address	D993B548h
Table Length	2850 bytes
OEM ID	FUJ
OEM Table ID	JIB75Y3
OEM Revision	40900000h
Creator ID	INTL
Creator Revision	20051117h

[XSDT: Extended System Description Table]

ACPI Table Properties:

ACPI Signature	XSDT
Table Description	Extended System Description Table
Memory Address	00000000-D9930080h
Table Length	132 bytes
OEM ID	FUJ
OEM Table ID	PC
OEM Revision	40900000h
Creator ID	AMI
Creator Revision	00010013h
XSDT Entry #0	00000000-D993A3E8h (FACP)
XSDT Entry #1	00000000-D993A4F8h (APIC)
XSDT Entry #2	00000000-D993A570h (FPDT)
XSDT Entry #3	00000000-D993A5B8h (MCFG)
XSDT Entry #4	00000000-D993A5F8h (MSDM)
XSDT Entry #5	00000000-D993A650h (BOOT)
XSDT Entry #6	00000000-D993A678h (HPET)
XSDT Entry #7	00000000-D993A6B0h (SSDT)
XSDT Entry #8	00000000-D993AA20h (SLIC)
XSDT Entry #9	00000000-D993AB98h (SSDT)
XSDT Entry #10	00000000-D993B548h (SSDT)
XSDT Entry #11	00000000-D993C070h (ASF!)

Operating System

Operating System Properties:

Navigation

OS Name	Microsoft Windows 10 Pro
OS Language	English (United States)
OS Installer Language	English (United States)
OS Kernel Type	Multiprocessor Free (64-bit)
OS Version	10.0.19042.508
OS Service Pack	[TRIAL VERSION]
OS Installation Date	9/8/2020
OS Root	C:\WINDOWS

License Information:

Registered Owner	bebosmj0@gmail.com
Registered Organization	
Product ID	00330-80000-00000-AA999
Product Key	VK7JG- [TRIAL VERSION]
Product Activation (WPA)	Not Required

Current Session:

Computer Name	VIETHOANG
User Name	bebos
Logon Domain	[TRIAL VERSION]
UpTime	7448 sec (0 days, 2 hours, 4 min, 8 sec)

Components Version:

Common Controls	6.16
Internet Explorer Updates	[TRIAL VERSION]
Windows Mail	-
Windows Media Player	-
Windows Messenger	-
MSN Messenger	-
Internet Information Services (IIS)	[TRIAL VERSION]
.NET Framework	4.8.4200.0 built by: NET48REL1LAST_C
Novell Client	-
DirectX	DirectX 12.0
OpenGL	10.0.19041.488 (WinBuild.160101.0800)
ASPI	-

Operating System Features:

Debug Version	No
DBCS Version	No
Domain Controller	No
Security Present	No
Network Present	Yes
Remote Session	No
Safe Mode	No
Slow Processor	No
Terminal Services	Yes

Processes

Process Name	Process File Name	Type	Used Memory	Used Swap
AcWebBrowser.exe	C:\Program Files (x86)\Autodesk\Autodesk Desktop App\acwebbrowser\acwebbrowser.exe	32-bit	29932 KB	17 KB
AcWebBrowser.exe	C:\Program Files (x86)\Autodesk\Autodesk Desktop App\acwebbrowser\acwebbrowser.exe	32-bit	29352 KB	7 KB
AcWebBrowser.exe	C:\Program Files (x86)\Autodesk\Autodesk Desktop App\acwebbrowser\acwebbrowser.exe	32-bit	42496 KB	26 KB

AdAppMgrSvc.exe	C:\Program Files (x86)\Autodesk\Autodesk Desktop App\AdAppMgrSvc.exe		8992 KB	4 KB
AdskLicensingService.exe	C:\Program Files (x86)\Common Files\Autodesk Shared\AdskLicensing\Current\AdskLicensingService\AdskLicensingService.exe	32-bit	3632 KB	9 KB
aida64.exe	C:\Program Files (x86)\FinalWire\AIDA64 Extreme\aida64.exe	32-bit	90 MB	73 KB
AppleMobileDeviceProcess.exe	C:\Program Files\WindowsApps\AppleInc.iTunes_12108.5.48031.0_x64__nzyj5cx40ttqa\AMDS64\AppleMobileDeviceProcess.exe	64-bit	12800 KB	3 KB
ApplicationFrameHost.exe	C:\WINDOWS\system32\ApplicationFrameHost.exe	64-bit	29320 KB	11 KB
audiodg.exe	C:\WINDOWS\system32\AUDIODG.EXE	64-bit	14236 KB	13 KB
AutodeskDesktopApp.exe	C:\Program Files (x86)\Autodesk\Autodesk Desktop App\AutodeskDesktopApp.exe	32-bit	28868 KB	16 KB
BtSwitcherService.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\BtSwitcherService.exe	64-bit	1704 KB	1 KB
conhost.exe	C:\WINDOWS\system32\conhost.exe	64-bit	1048 KB	6 KB
Cortana.exe	C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_2.2009.2711.0_x64__8wekyb3d8bbwe\Cortana.exe	64-bit	80860 KB	38 KB
CsrAudioguiCtrl.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrAudioguiCtrl.exe	64-bit	8864 KB	1 KB
CsrBtAudioService.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrBtAudioService.exe	64-bit	3932 KB	2 KB
CsrBtOBEXService.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrBtOBEXService.exe	64-bit	4504 KB	9 KB
CsrBtService.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrBtService.exe	64-bit	4700 KB	3 KB
CsrHCRPServer.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrHCRPServer.exe	64-bit	10988 KB	2 KB
csrss.exe		64-bit	6012 KB	2 KB
csrss.exe		64-bit	3032 KB	1 KB
CsrSyncMLServer.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrSyncMLServer.exe	64-bit	8924 KB	1 KB
ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe	64-bit	24020 KB	6 KB
dllhost.exe	C:\WINDOWS\system32\DllHost.exe	64-bit	7068 KB	1 KB
dllhost.exe	C:\WINDOWS\system32\DllHost.exe	64-bit	12588 KB	4 KB
dllhost.exe	C:\WINDOWS\system32\DllHost.exe	64-bit	2180 KB	2 KB
dwm.exe	C:\WINDOWS\System32\dwm.exe	64-bit	61592 KB	52 KB
explorer.exe	C:\WINDOWS\Explorer.EXE	64-bit	109 MB	46 KB
FNPLicensingService.exe	C:\Program Files (x86)\Common Files\Macrovision Shared\FlexNet Publisher\FNPLicensingService.exe	32-bit	2540 KB	2 KB
fontdrvhost.exe	C:\WINDOWS\System32\fontdrvhost.exe	64-bit	7360 KB	3 KB
fontdrvhost.exe	C:\WINDOWS\system32\fontdrvhost.exe	64-bit	152 KB	1 KB
fuj02e3-utility.exe	C:\WINDOWS\System32\DriverStore\FileRepository\fuj02e3.inf_amd64_42f2ff7fcce64487\fuj02e3-utility.exe	64-bit	2324 KB	1 KB
GenuineService.exe	C:\Users\bebos\AppData\Local\Programs\Autodesk\Genuine Service\GenuineService.exe	32-bit	11928 KB	3 KB
HarmonyUserStartup.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\HarmonyUserStartup.exe	64-bit	8556 KB	1 KB
igfxCUIService.exe	C:\WINDOWS\system32\igfxCUIService.exe	64-bit	4244 KB	1 KB
igfxEM.exe	C:\WINDOWS\system32\igfxEM.exe	64-bit	13368 KB	7 KB
igfxHK.exe	C:\WINDOWS\system32\igfxHK.exe	64-bit	11040 KB	5 KB
igfxTray.exe	C:\WINDOWS\system32\igfxTray.exe	64-bit	12120 KB	7 KB
jusched.exe	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	32-bit	7660 KB	1 KB
Krisp.exe	C:\Program Files\Krisp\Krisp.exe	64-bit	83612 KB	115 KB
LockApp.exe	C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe	64-bit	36856 KB	13 KB
lsass.exe	C:\WINDOWS\system32\lsass.exe	64-bit	17388 KB	9 KB
Memory Compression		64-bit	110 MB	0 KB
Messenger.exe	C:\Program Files\WindowsApps\FACEBOOK.317180B0BB486_640.5.121.0_x64__8xx8rvfyw5nnt\app\Messenger.exe	64-bit	79556 KB	36 KB
Messenger.exe	C:\Program Files\WindowsApps\FACEBOOK.317180B0BB486_640.5.121.0_x64__8xx8rvfyw5nnt\app\Messenger.exe	64-bit	37804 KB	12 KB
Messenger.exe	C:\Program Files\WindowsApps\FACEBOOK.317180B0BB486_640.5.121.0_x64__8xx8rvfyw5nnt\app\Messenger.exe	64-bit	175 MB	144 KB
Messenger.exe	C:\Program Files\WindowsApps\FACEBOOK.317180B0BB486_640.5.121.0_x64__8xx8rvfyw5nnt\app\Messenger.exe	64-bit	68468 KB	29 KB
Messenger.exe	C:\Program Files\WindowsApps\FACEBOOK.317180B0BB486_640.5.121.0_x64__8xx8rvfyw5nnt\app\Messenger.exe	64-bit	24748 KB	9 KB
Messenger.exe	C:\Program Files\WindowsApps\FACEBOOK.317180B0BB486_640.5.121.0_x64__8xx8rvfyw5nnt\app\Messenger.exe	64-bit	111 MB	90 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	39092 KB	15 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	42428 KB	18 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	24328 KB	10 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	6864 KB	1 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	18944 KB	5 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	178 MB	148 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	161 MB	67 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	612 MB	573 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	43740 KB	19 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	64-bit	31960 KB	15 KB

msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Navigation		76584 KB	47 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		64-bit	71736 KB	41 KB
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		64-bit	19276 KB	7 KB
MsMpEng.exe			64-bit	119 MB	198 KB
NisSrv.exe			64-bit	5432 KB	6 KB
OfficeClickToRun.exe	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe		64-bit	23200 KB	34 KB
OneDrive.exe	C:\Users\bebos\AppData\Local\Microsoft\OneDrive\OneDrive.exe		32-bit	54796 KB	20 KB
PresentationFontCache.exe	C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe		64-bit	2400 KB	23 KB
RAVCpl64.exe	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe		64-bit	13812 KB	4 KB
register-service.exe	C:\Program Files\Chaos Group\V-Ray\Swarm 1.4\register-service.exe		32-bit	1348 KB	3 KB
Registry			64-bit	45332 KB	7 KB
remoting_host.exe	C:\Program Files (x86)\Google\Chrome Remote Desktop\85.0.4183.6\remoting_host.exe		32-bit	3404 KB	4 KB
remoting_host.exe	C:\Program Files (x86)\Google\Chrome Remote Desktop\85.0.4183.6\remoting_host.exe		32-bit	13316 KB	9 KB
rundll32.exe	C:\WINDOWS\System32\rundll32.exe		64-bit	10168 KB	1 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	20388 KB	3 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	29860 KB	8 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	6788 KB	1 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	37516 KB	11 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	28672 KB	7 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	27844 KB	6 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	16252 KB	3 KB
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe		64-bit	21120 KB	5 KB
SearchApp.exe	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe		64-bit	80132 KB	90 KB
SearchIndexer.exe	C:\WINDOWS\system32\SearchIndexer.exe		64-bit	21376 KB	24 KB
SecurityHealthService.exe			64-bit	7780 KB	3 KB
SecurityHealthSystray.exe	C:\Windows\System32\SecurityHealthSystray.exe		64-bit	8976 KB	1 KB
services.exe			64-bit	6052 KB	5 KB
SettingSyncHost.exe	C:\WINDOWS\system32\SettingSyncHost.exe		64-bit	5576 KB	2 KB
SgrmBroker.exe			64-bit	5068 KB	5 KB
ShellExperienceHost.exe	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe		64-bit	44284 KB	15 KB
sihost.exe	C:\WINDOWS\system32\sihost.exe		64-bit	25292 KB	6 KB
smartscreen.exe	C:\Windows\System32\smartscreen.exe		64-bit	22692 KB	7 KB
smss.exe			64-bit	352 KB	1 KB
SpeechRuntime.exe	C:\Windows\System32\Speech_OneCore\Common\SpeechRuntime.exe		64-bit	18764 KB	4 KB
splwow64.exe	C:\WINDOWS\splwow64.exe		64-bit	11720 KB	2 KB
spoolsv.exe	C:\WINDOWS\System32\spoolsv.exe		64-bit	4992 KB	5 KB
sppsvc.exe			64-bit	13724 KB	4 KB
StartMenuExperienceHost.exe	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe		64-bit	67996 KB	22 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	4908 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	16308 KB	8 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	2272 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	5260 KB	2 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	4784 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4088 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	8504 KB	5 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	26256 KB	10 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	7192 KB	4 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	1816 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3752 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4408 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	7672 KB	3 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	1880 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	13080 KB	14 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4120 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	5736 KB	2 KB

svchost.exe	C:\WINDOWS\System32\svchost.exe	Navigation		1264 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	2668 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4900 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3236 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	3948 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	8464 KB	4 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	19196 KB	30 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	2300 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3492 KB	4 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3132 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3616 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4576 KB	3 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	9932 KB	5 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	7392 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	6668 KB	3 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	10792 KB	7 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4796 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	7488 KB	9 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	2516 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	8500 KB	4 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	20264 KB	16 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3580 KB	2 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	7604 KB	4 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	1144 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	2980 KB	2 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	1504 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	14336 KB	4 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	12292 KB	4 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	1104 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	2120 KB	2 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	2900 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	5412 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	8684 KB	3 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	1652 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	5108 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	13112 KB	7 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	1824 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4348 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3336 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	12208 KB	9 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	5884 KB	3 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	6052 KB	7 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	3692 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	13500 KB	5 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4008 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	5304 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	3020 KB	2 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	5196 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	4868 KB	2 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		64-bit	7076 KB	5 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	5180 KB	2 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	7964 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	660 KB	0 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	22152 KB	8 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe		64-bit	12504 KB	2 KB

svchost.exe	C:\WINDOWS\system32\svchost.exe		3696 KB	1 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe		5336 KB	1 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe	64-bit	18780 KB	11 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe	64-bit	35876 KB	8 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe	64-bit	6968 KB	4 KB
svchost.exe	C:\WINDOWS\system32\svchost.exe	64-bit	17284 KB	3 KB
svchost.exe	C:\WINDOWS\System32\svchost.exe	64-bit	20996 KB	9 KB
swrm.exe	C:\Program Files\Chaos Group\V-Ray\Swarm 1.4\swrm.exe	64-bit	11360 KB	59 KB
System Idle Process			8 KB	0 KB
System		64-bit	24 KB	0 KB
SystemSettings.exe	C:\Windows\ImmersiveControlPanel\SystemSettings.exe	64-bit	1456 KB	23 KB
taskhostw.exe	C:\WINDOWS\system32\taskhostw.exe	64-bit	3892 KB	3 KB
taskhostw.exe	C:\WINDOWS\system32\taskhostw.exe	64-bit	17680 KB	7 KB
TextInputHost.exe	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe	64-bit	38300 KB	14 KB
TrayApplication.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\TrayApplication.exe	64-bit	10056 KB	2 KB
UserOOBEBroker.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe	64-bit	8860 KB	1 KB
vksts.exe	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\vksts.exe	64-bit	8068 KB	1 KB
vrol.exe	C:\Program Files\Chaos Group\VRLService\OLS\vrol.exe	64-bit	10596 KB	22 KB
Win32Bridge.Server.exe	C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_2.2009.2711.0_x64__8wekyb3d8bbwe\Win32Bridge.Server.exe	64-bit	34840 KB	10 KB
wininit.exe		64-bit	2992 KB	1 KB
winlogon.exe	C:\WINDOWS\System32\WinLogon.exe	64-bit	9840 KB	2 KB
WinStore.App.exe	C:\Program Files\WindowsApps\Microsoft.WindowsStore_12009.1001.1.0_x64__8wekyb3d8bbwe\WinStore.App.exe	64-bit	1760 KB	47 KB
WmiPrvSE.exe	C:\WINDOWS\sysWOW64\wbem\wmiprvse.exe	64-bit	11176 KB	3 KB
WmiPrvSE.exe	C:\WINDOWS\system32\wbem\wmiprvse.exe	64-bit	9380 KB	2 KB
WmiPrvSE.exe	C:\WINDOWS\system32\wbem\wmiprvse.exe	64-bit	11676 KB	4 KB
WUDFHost.exe	C:\Windows\System32\WUDFHost.exe	64-bit	1552 KB	1 KB
YourPhone.exe	C:\Program Files\WindowsApps\Microsoft.YourPhone_1.20082.139.0_x64__8wekyb3d8bbwe\YourPhone.exe	64-bit	2044 KB	23 KB

System Drivers

Driver Name	Driver Description	File Name	Version	Type	State
1394ohci	1394 OHCI Compliant Host Controller	1394ohci.sys	10.0.19041.1	Kernel Driver	Stopped
3ware	3ware	3ware.sys	5.1.0.51	Kernel Driver	Stopped
ACPI	Microsoft ACPI Driver	ACPI.sys	10.0.19041.488	Kernel Driver	Running
AcpiDev	ACPI Devices driver	AcpiDev.sys	10.0.19041.1	Kernel Driver	Stopped
acpiex	Microsoft ACPIEx Driver	acpiex.sys	10.0.19041.1	Kernel Driver	Running
acpipagr	ACPI Processor Aggregator Driver	acpipagr.sys	10.0.19041.1	Kernel Driver	Stopped
AcpiPmi	ACPI Power Meter Driver	acpipmi.sys	10.0.19041.1	Kernel Driver	Stopped
acpitime	ACPI Wake Alarm Driver	acpitime.sys	10.0.19041.1	Kernel Driver	Stopped
Acx01000	Acx01000	Acx01000.sys	10.0.19041.1	Kernel Driver	Stopped
ADP80XX	ADP80XX	ADP80XX.SYS	1.3.0.10769	Kernel Driver	Stopped
AFD	Ancillary Function Driver for Winsock	afd.sys	10.0.19041.488	Kernel Driver	Running
afunix	afunix	afunix.sys	10.0.19041.488	Kernel Driver	Running
ahcache	Application Compatibility Cache	ahcache.sys	10.0.19041.1	Kernel Driver	Running
AIDA64Driver	FinalWire AIDA64 Kernel Driver	kerneld.x64		Kernel Driver	Running
amdgpio2	AMD GPIO Client Driver	amdgpio2.sys	2.2.0.71	Kernel Driver	Stopped
amdi2c	AMD I2C Controller Service	amdi2c.sys	1.2.0.99	Kernel Driver	Stopped
AmdK8	AMD K8 Processor Driver	amdk8.sys	10.0.19041.1	Kernel Driver	Stopped
AmdPPM	AMD Processor Driver	amdppm.sys	10.0.19041.1	Kernel Driver	Stopped
amdsata	amdsata	amdsata.sys	1.1.3.277	Kernel Driver	Stopped
amdsbs	amdsbs	amdsbs.sys	3.7.1540.43	Kernel Driver	Stopped
amdxata	amdxata	amdxata.sys	1.1.3.277	Kernel Driver	Stopped
AppID	AppID Driver	appid.sys	10.0.19041.488	Kernel Driver	Stopped

applockerfltr	Smartlocker Filter Driver	applockerfltr.sys	1.488	Kernel Driver	Stopped
AppvStrm	AppvStrm	AppvStrm.sys	10.0.19041.1	File System Driver	Stopped
AppvVemgr	AppvVemgr	AppvVemgr.sys	10.0.19041.1	File System Driver	Stopped
AppvVfs	AppvVfs	AppvVfs.sys	10.0.19041.1	File System Driver	Stopped
arcsas	Adaptec SAS/SATA-II RAID Storport's Miniport Driver	arcsas.sys	7.5.0.32048	Kernel Driver	Stopped
AsyncMac	RAS Asynchronous Media Driver	asyncmac.sys	10.0.19041.1	Kernel Driver	Running
atapi	IDE Channel	atapi.sys	10.0.19041.488	Kernel Driver	Stopped
b06bdrv	QLogic Network Adapter VBD	bxvbda.sys	7.12.31.105	Kernel Driver	Stopped
bam	Background Activity Moderator Driver	bam.sys	10.0.19041.1	Kernel Driver	Running
BasicDisplay	BasicDisplay	BasicDisplay.sys	10.0.19041.1	Kernel Driver	Running
BasicRender	BasicRender	BasicRender.sys	10.0.19041.84	Kernel Driver	Running
bcmfn2	bcmfn2 Service	bcmfn2.sys	6.3.9600.17336	Kernel Driver	Stopped
Beep	Beep			Kernel Driver	Running
bindflt	Windows Bind Filter Driver	bindflt.sys	10.0.19041.292	File System Driver	Running
bowser	Browser	bowser.sys	10.0.19041.1	File System Driver	Running
BthA2dp	Microsoft Bluetooth A2dp driver	BthA2dp.sys	10.0.19041.487	Kernel Driver	Stopped
BthEnum	Bluetooth Enumerator Service	BthEnum.sys	10.0.19041.488	Kernel Driver	Stopped
BthHFEnum	Microsoft Bluetooth Hands-Free Profile driver	bthhfenum.sys	10.0.19041.1	Kernel Driver	Stopped
BthLEEnum	Bluetooth Low Energy Driver	Microsoft.Bluetooth.Legacy.LEEnumerator.sys	10.0.19041.488	Kernel Driver	Stopped
BthMini	Bluetooth Radio Driver	BTHMINI.sys	10.0.19041.488	Kernel Driver	Stopped
BTHMODEM	Bluetooth Modem Communications Driver	bthmodem.sys	10.0.19041.1	Kernel Driver	Stopped
BTHPORT	Bluetooth Port Driver	BTHport.sys	10.0.19041.488	Kernel Driver	Stopped
BTHUSB	Bluetooth Radio USB Driver	BTHUSB.sys	10.0.19041.488	Kernel Driver	Stopped
bttflt	Microsoft Hyper-V VHDPMEM BTT Filter	bttflt.sys	10.0.19041.1	Kernel Driver	Stopped
buttonconverter	Service for Portable Device Control devices	buttonconverter.sys	10.0.19041.1	Kernel Driver	Stopped
CAD	Charge Arbitration Driver	CAD.sys	10.0.19041.1	Kernel Driver	Stopped
cdfs	CD/DVD File System Reader	cdfs.sys	10.0.19041.1	File System Driver	Stopped
cdrom	CD-ROM Driver	cdrom.sys	10.0.19041.1	Kernel Driver	Running
cht4iscsi	cht4iscsi	cht4sx64.sys	6.11.4.100	Kernel Driver	Stopped
cht4vbd	Chelsio Virtual Bus Driver	cht4vx64.sys	6.11.4.100	Kernel Driver	Stopped
CimFS	CimFS			File System Driver	Running
circlass	Consumer IR Devices	circlass.sys	10.0.19041.1	Kernel Driver	Stopped
CldFlt	Windows Cloud Files Filter Driver	cldflt.sys	10.0.19041.488	File System Driver	Running
CLFS	Common Log (CLFS)	CLFS.sys	10.0.19041.508	Kernel Driver	Running
CmBatt	Microsoft ACPI Control Method Battery Driver	CmBatt.sys	10.0.19041.1	Kernel Driver	Stopped
CNG	CNG	cng.sys	10.0.19041.264	Kernel Driver	Running
cnghwassist	CNG Hardware Assist algorithm provider	cnghwassist.sys	10.0.19041.1	Kernel Driver	Stopped
CompositeBus	Composite Bus Enumerator Driver	CompositeBus.sys	10.0.19041.1	Kernel Driver	Running
condrv	Console Driver	condrv.sys	10.0.19041.1	Kernel Driver	Running
CSC	Offline Files Driver	csc.sys	10.0.19041.1	Kernel Driver	Running
csr_bthav	Bluetooth AV Profile	csrbthav.sys	2.1.60.0	Kernel Driver	Running
csravrcp	Bluetooth AVRCP Profile	csravrcp.sys	2.1.51.0	Kernel Driver	Running
CsrBthAudioHF	BthAudioHF Service	CsrBthAudioHF.sys	2.1.60.0	Kernel Driver	Running
CsrBtPort	Csr Bluetooth Device Driver	CsrBtPort.sys	2.1.61.0	Kernel Driver	Running
csrhfgcc	Bluetooth HFG Call Control Profile	csrhfgcc.sys	2.1.52.0	Kernel Driver	Running
csrhidmini	Bluetooth HID Host Profile	csrhidmini.sys	2.1.60.0	Kernel Driver	Stopped
csrpan	Bluetooth Personal Area Network Device Driver	csrpan.sys	2.1.51.0	Kernel Driver	Running
csrserial	SPP Device Driver	csrserial.sys	2.1.51.0	Kernel Driver	Running
csrusb	CSR USB driver for Bluetooth dongle	csrusb.sys	2.1.60.0	Kernel Driver	Running
csrusbfilter	CSR USB filter driver	csrusbfilter.sys	2.1.60.0	Kernel Driver	Running
dam	Desktop Activity Moderator Driver	dam.sys	10.0.19041.1	Kernel Driver	Stopped
Dfsc	DFS Namespace Client Driver	dfsc.sys	10.0.19041.1	File System Driver	Running
dg_ssudbus	SAMSUNG Mobile USB Composite Device Driver (DEVGURU Ver.)	ssudbus.sys	2.16.15.0	Kernel Driver	Running
disk	Disk Driver	disk.sys	10.0.19041.1	Kernel Driver	Running
dmvsc	dmvsc	dmvsc.sys	10.0.19041.1	Kernel Driver	Stopped

drmkaud	Microsoft Trusted Audio Drivers	drmkaud.sys	1.1	Kernel Driver	Stopped
DXGKrnl	LDDM Graphics Subsystem	dxgkrnl.sys	10.0.19041.508	Kernel Driver	Running
ebdrv	QLogic 10 Gigabit Ethernet Adapter VBD	evbda.sys	7.13.65.105	Kernel Driver	Stopped
EhStorClass	Enhanced Storage Filter Driver	EhStorClass.sys	10.0.19041.1	Kernel Driver	Running
EhStorTcgDrv	Microsoft driver for storage devices supporting IEEE 1667 and TCG protocols	EhStorTcgDrv.sys	10.0.19041.1	Kernel Driver	Stopped
ErrDev	Microsoft Hardware Error Device Driver	errdev.sys	10.0.19041.1	Kernel Driver	Stopped
exfat	exFAT File System Driver			File System Driver	Stopped
fastfat	FAT12/16/32 File System Driver			File System Driver	Stopped
fdc	Floppy Disk Controller Driver	fdc.sys	10.0.19041.1	Kernel Driver	Stopped
FileCrypt	FileCrypt	filecrypt.sys	10.0.19041.1	File System Driver	Running
FileInfo	File Information FS MiniFilter	fileinfo.sys	10.0.19041.1	File System Driver	Running
Filetrace	Filetrace	filetrace.sys	10.0.19041.1	File System Driver	Stopped
flpydisk	Floppy Disk Driver	flpydisk.sys	10.0.19041.1	Kernel Driver	Stopped
FltMgr	FltMgr	fltmgr.sys	10.0.19041.264	File System Driver	Running
FsDepends	File System Dependency Minifilter	FsDepends.sys	10.0.19041.1	File System Driver	Stopped
fuj02e3	Fujitsu FUJ02E3 Device Driver Service	fuj02e3.sys	4.3.0.0	Kernel Driver	Running
fvevol	BitLocker Drive Encryption Filter Driver	fvevol.sys	10.0.19041.1	Kernel Driver	Running
gameflt	gameflt	gameflt.sys	10.0.19041.3952	File System Driver	Stopped
gencounter	Microsoft Hyper-V Generation Counter	vmgencounter.sys	10.0.19041.1	Kernel Driver	Stopped
genericusbfn	Generic USB Function Class	genericusbfn.sys	10.0.19041.1	Kernel Driver	Stopped
GPIOClx0101	Microsoft GPIO Class Extension Driver	msgpioclx.sys	10.0.19041.488	Kernel Driver	Stopped
GpuEnergyDrv	GPU Energy Driver	gpuenergydrv.sys	10.0.19041.1	Kernel Driver	Running
HdAudAddService	Microsoft 1.1 UAA Function Driver for High Definition Audio Service	HdAudio.sys	10.0.19041.264	Kernel Driver	Stopped
HDAudBus	Microsoft UAA Bus Driver for High Definition Audio	HDAudBus.sys	10.0.19041.1	Kernel Driver	Running
HidBatt	HID UPS Battery Driver	HidBatt.sys	10.0.19041.1	Kernel Driver	Stopped
HidBth	Microsoft Bluetooth HID Miniport	hidbth.sys	10.0.19041.423	Kernel Driver	Stopped
hidi2c	Microsoft I2C HID Miniport Driver	hidi2c.sys	10.0.19041.1	Kernel Driver	Stopped
hidinterrupt	Common Driver for HID Buttons implemented with interrupts	hidinterrupt.sys	10.0.19041.1	Kernel Driver	Stopped
HidIr	Microsoft Infrared HID Driver	hidir.sys	10.0.19041.1	Kernel Driver	Stopped
hidspi	Microsoft SPI HID Miniport Driver	hidspi.sys	10.0.19041.1	Kernel Driver	Stopped
HidUsb	Microsoft HID Class Driver	hidusb.sys	10.0.19041.1	Kernel Driver	Running
HpSAMD	HpSAMD	HpSAMD.sys	8.0.4.0	Kernel Driver	Stopped
HTTP	HTTP Service	HTTP.sys	10.0.19041.1	Kernel Driver	Running
hvcrash	hvcrash	hvcrash.sys	10.0.19041.1	Kernel Driver	Stopped
hvservice	Hypervisor/Virtual Machine Support Driver	hvservice.sys	10.0.19041.508	Kernel Driver	Stopped
HwNClx0101	Microsoft Hardware Notifications Class Extension Driver	mshwnclx.sys	10.0.19041.1	Kernel Driver	Stopped
hwpolicy	Hardware Policy Driver	hwpolicy.sys	10.0.19041.423	Kernel Driver	Stopped
hyperkbd	hyperkbd	hyperkbd.sys	10.0.19041.1	Kernel Driver	Stopped
HyperVideo	HyperVideo	HyperVideo.sys	10.0.19041.1	Kernel Driver	Stopped
i8042prt	i8042 Keyboard and PS/2 Mouse Port Driver	i8042prt.sys	10.0.19041.1	Kernel Driver	Stopped
iagpio	Intel Serial IO GPIO Controller Driver	iagpio.sys	1.1.1.0	Kernel Driver	Stopped
iai2c	Intel(R) Serial IO I2C Host Controller	iai2c.sys	1.1.1.0	Kernel Driver	Stopped
iaLPSS2i_GPIO2_BXT_P	Intel(R) Serial IO GPIO Driver v2	iaLPSS2i_GPIO2_BXT_P.sys	30.100.1816.1	Kernel Driver	Stopped
iaLPSS2i_GPIO2_CNL	Intel(R) Serial IO GPIO Driver v2	iaLPSS2i_GPIO2_CNL.sys	30.100.1816.3	Kernel Driver	Stopped
iaLPSS2i_GPIO2_GLK	Intel(R) Serial IO GPIO Driver v2	iaLPSS2i_GPIO2_GLK.sys	30.100.1820.1	Kernel Driver	Stopped
iaLPSS2i_GPIO2	Intel(R) Serial IO GPIO Driver v2	iaLPSS2i_GPIO2.sys	30.100.1816.3	Kernel Driver	Stopped
iaLPSS2i_I2C_BXT_P	Intel(R) Serial IO I2C Driver v2	iaLPSS2i_I2C_BXT_P.sys	30.100.1816.1	Kernel Driver	Stopped
iaLPSS2i_I2C_CNL	Intel(R) Serial IO I2C Driver v2	iaLPSS2i_I2C_CNL.sys	30.100.1929.1	Kernel Driver	Stopped
iaLPSS2i_I2C_GLK	Intel(R) Serial IO I2C Driver v2	iaLPSS2i_I2C_GLK.sys	30.100.1820.1	Kernel Driver	Stopped
iaLPSS2i_I2C	Intel(R) Serial IO I2C Driver v2	iaLPSS2i_I2C.sys	30.100.1816.3	Kernel Driver	Stopped
iaLPSSi_GPIO	Intel(R) Serial IO GPIO Controller Driver	iaLPSSi_GPIO.sys	1.1.250.0	Kernel Driver	Stopped
iaLPSSi_I2C	Intel(R) Serial IO I2C Controller Driver	iaLPSSi_I2C.sys	1.1.253.0	Kernel Driver	Stopped
iaStorAVC	Intel Chipset SATA RAID Controller	iaStorAVC.sys	15.44.0.1015	Kernel Driver	Stopped
iaStorV	Intel RAID Controller Windows 7	iaStorV.sys	8.6.2.1019	Kernel Driver	Stopped
ibbus	Mellanox InfiniBand Bus/AL (Filter Driver)	ibbus.sys	5.50.14695.0	Kernel Driver	Stopped

igfx	igfx	igdkmd64.sys	Navigation 5129	Kernel Driver	Running
IndirectKmd	Indirect Displays Kernel-Mode Driver	IndirectKmd.sys	10.0.19041.1	Kernel Driver	Stopped
IntcAzAudAddService	Service for Realtek HD Audio (WDM)	RTKVHD64.sys	6.0.8746.1	Kernel Driver	Running
intelide	intelide	intelide.sys	10.0.19041.488	Kernel Driver	Stopped
intelpep	Intel(R) Power Engine Plug-in Driver	intelpep.sys	10.0.19041.488	Kernel Driver	Running
intelpmax	Intel(R) Dynamic Device Peak Power Manager Driver	intelpmax.sys	10.0.19041.1	Kernel Driver	Stopped
intelppm	Intel Processor Driver	intelppm.sys	10.0.19041.1	Kernel Driver	Running
iorate	Disk I/O Rate Filter Driver	iorate.sys	10.0.19041.1	Kernel Driver	Running
IpFilterDriver	IP Traffic Filter Driver	ipfltdrv.sys	10.0.19041.1	Kernel Driver	Stopped
IPMIDRV	IPMIDRV	IPMIDrv.sys	10.0.19041.1	Kernel Driver	Stopped
IPNAT	IP Network Address Translator	ipnat.sys	10.0.19041.1	Kernel Driver	Stopped
IPT	IPT	ipt.sys	10.0.19041.1	Kernel Driver	Stopped
isapnp	isapnp	isapnp.sys	10.0.19041.1	Kernel Driver	Stopped
iScsiPrt	iScsiPort Driver	msiscsi.sys	10.0.19041.1	Kernel Driver	Stopped
ItSas35i	ItSas35i	ItSas35i.sys	2.60.94.80	Kernel Driver	Stopped
iwdbus	IWD Bus Enumerator	iwdbus.sys	4.5.71.0	Kernel Driver	Stopped
kbdclass	Keyboard Class Driver	kbdclass.sys	10.0.19041.1	Kernel Driver	Running
kbdhid	Keyboard HID Driver	kbdhid.sys	10.0.19041.1	Kernel Driver	Running
kdnic	Microsoft Kernel Debug Network Miniport (NDIS 6.20)	kdnic.sys	6.1.0.0	Kernel Driver	Running
KrispSimple	Krisp	KrispVad.sys		Kernel Driver	Running
KSecDD	KSecDD	ksecdd.sys	10.0.19041.488	Kernel Driver	Running
KSecPkg	KSecPkg	ksecpkg.sys	10.0.19041.508	Kernel Driver	Running
ksthunk	Kernel Streaming Thunks	ksthunk.sys	10.0.19041.1	Kernel Driver	Running
lltdio	Link-Layer Topology Discovery Mapper I/O Driver	lltdio.sys	10.0.19041.1	Kernel Driver	Running
LSI_SAS	LSI_SAS	lsi_sas.sys	1.34.3.83	Kernel Driver	Stopped
LSI_SAS2i	LSI_SAS2i	lsi_sas2i.sys	2.0.79.82	Kernel Driver	Stopped
LSI_SAS3i	LSI_SAS3i	lsi_sas3i.sys	2.51.26.80	Kernel Driver	Stopped
LSI_SSS	LSI_SSS	lsi_sss.sys	2.10.61.81	Kernel Driver	Stopped
luafv	UAC File Virtualization	luafv.sys	10.0.19041.1	File System Driver	Running
mausbhost	MA-USB Host Controller Driver	mausbhost.sys	10.0.19041.1	Kernel Driver	Stopped
mausbip	MA-USB IP Filter Driver	mausbip.sys	10.0.19041.1	Kernel Driver	Stopped
MbbCx	MBB Network Adapter Class Extension	MbbCx.sys	10.0.19041.423	Kernel Driver	Stopped
megasas	megasas	megasas.sys	6.706.6.0	Kernel Driver	Stopped
megasas2i	megasas2i	MegaSas2i.sys	6.714.20.0	Kernel Driver	Stopped
megasas35i	megasas35i	megasas35i.sys	7.710.10.0	Kernel Driver	Stopped
megasr	megasr	megasr.sys	15.2.2013.129	Kernel Driver	Stopped
MEIx64	Intel(R) Management Engine Interface	TeeDriverW8x64.sys	11.0.5.1189	Kernel Driver	Running
Microsoft_Bluetooth_AvrcpTransport	Microsoft Bluetooth Avrcp Transport Driver	Microsoft.Bluetooth.AvrcpTransport.sys	10.0.19041.1	Kernel Driver	Stopped
mlx4_bus	Mellanox ConnectX Bus Enumerator	mlx4_bus.sys	5.50.14695.0	Kernel Driver	Stopped
MMCSS	Multimedia Class Scheduler	mmcss.sys	10.0.19041.1	Kernel Driver	Running
Modem	Modem	modem.sys	10.0.19041.1	Kernel Driver	Running
monitor	Microsoft Monitor Class Function Driver Service	monitor.sys	10.0.19041.488	Kernel Driver	Running
mouclass	Mouse Class Driver	mouclass.sys	10.0.19041.1	Kernel Driver	Running
mouhid	Mouse HID Driver	mouhid.sys	10.0.19041.1	Kernel Driver	Running
mountmgr	Mount Point Manager	mountmgr.sys	10.0.19041.1	Kernel Driver	Running
mpsdrv	Windows Defender Firewall Authorization Driver	mpsdrv.sys	10.0.19041.1	Kernel Driver	Running
MRxDAV	WebDav Client Redirector Driver	mrxdav.sys	10.0.19041.1	File System Driver	Stopped
mrxsmb	SMB MiniRedirector Wrapper and Engine	mrxsmb.sys	10.0.19041.488	File System Driver	Running
mrxsmb20	SMB 2.0 MiniRedirector	mrxsmb20.sys	10.0.19041.488	File System Driver	Running
MsBridge	Microsoft MAC Bridge	bridge.sys	10.0.19041.1	Kernel Driver	Stopped
Msfs	Msfs			File System Driver	Running
msgpiowin32	Common Driver for Buttons, DockMode and Laptop/Slate Indicator	msgpiowin32.sys	10.0.19041.1	Kernel Driver	Stopped
mshidkmdf	Pass-through HID to KMDF Filter Driver	mshidkmdf.sys	10.0.19041.1	Kernel Driver	Stopped
mshidumdf	Pass-through HID to UMDF Driver	mshidumdf.sys	10.0.19041.1	Kernel Driver	Stopped
msisadrv	msisadrv	msisadrv.sys	10.0.19041.1	Kernel Driver	Running

MSKSSRV	Microsoft Streaming Service Proxy	MSKSSRV.sys	Navigation	1.1	Kernel Driver	Stopped
MsLldp	Microsoft Link-Layer Discovery Protocol	mslldp.sys		10.0.19041.1	Kernel Driver	Running
MSPCLOCK	Microsoft Streaming Clock Proxy	MSPCLOCK.sys		10.0.19041.1	Kernel Driver	Stopped
MSPQM	Microsoft Streaming Quality Manager Proxy	MSPQM.sys		10.0.19041.1	Kernel Driver	Stopped
MsQuic	MsQuic	msquic.sys		10.0.19041.488	Kernel Driver	Running
MsRPC	MsRPC				Kernel Driver	Stopped
MsSecFlt	Microsoft Security Events Component Minifilter	mssecflt.sys		10.0.19041.423	Kernel Driver	Running
mssmbios	Microsoft System Management BIOS Driver	mssmbios.sys		10.0.19041.1	Kernel Driver	Running
MSTEE	Microsoft Streaming Tee/Sink-to-Sink Converter	MSTEE.sys		10.0.19041.1	Kernel Driver	Stopped
MTConfig	Microsoft Input Configuration Driver	MTConfig.sys		10.0.19041.1	Kernel Driver	Stopped
Mup	Mup	mup.sys		10.0.19041.1	File System Driver	Running
mvumis	mvumis	mvumis.sys		1.0.5.1016	Kernel Driver	Stopped
NativeWifiP	NativeWiFi Filter	nwifi.sys		10.0.19041.488	Kernel Driver	Stopped
ndfltr	NetworkDirect Service	ndfltr.sys		5.50.14695.0	Kernel Driver	Stopped
NDIS	NDIS System Driver	ndis.sys		10.0.19041.488	Kernel Driver	Running
NdisCap	Microsoft NDIS Capture	ndiscap.sys		10.0.19041.1	Kernel Driver	Running
NdisImPlatform	Microsoft Network Adapter Multiplexor Protocol	NdisImPlatform.sys		10.0.19041.1	Kernel Driver	Stopped
NdisTapi	Remote Access NDIS TAPI Driver	ndistapi.sys		10.0.19041.1	Kernel Driver	Running
Ndisuio	NDIS Usermode I/O Protocol	ndisuio.sys		10.0.19041.1	Kernel Driver	Stopped
NdisVirtualBus	Microsoft Virtual Network Adapter Enumerator	NdisVirtualBus.sys		10.0.19041.1	Kernel Driver	Running
NdisWan	Remote Access NDIS WAN Driver	ndiswan.sys		10.0.19041.488	Kernel Driver	Running
ndiswanlegacy	Remote Access LEGACY NDIS WAN Driver	ndiswan.sys		10.0.19041.488	Kernel Driver	Stopped
NDKPing	NDKPing Driver	NDKPing.sys		10.0.19041.1	Kernel Driver	Stopped
ndproxy	NDIS Proxy Driver	NDProxy.sys		10.0.19041.1	Kernel Driver	Running
Ndu	Windows Network Data Usage Monitoring Driver	Ndu.sys		10.0.19041.1	Kernel Driver	Running
NetAdapterCx	Network Adapter Wdf Class Extension Library	NetAdapterCx.sys		10.0.19041.1	Kernel Driver	Stopped
NetBIOS	NetBIOS Interface	netbios.sys		10.0.19041.1	File System Driver	Running
NetBT	NetBT	netbt.sys		10.0.19041.1	Kernel Driver	Running
netvsc	netvsc	netvsc.sys		10.0.19041.1	Kernel Driver	Stopped
Npfs	Npfs				File System Driver	Running
npsvctrig	Named pipe service trigger provider	npsvctrig.sys		10.0.19041.1	Kernel Driver	Running
nsiproxy	NSI Proxy Service Driver	nsiproxy.sys		10.0.19041.1	Kernel Driver	Running
Ntfs	Ntfs				File System Driver	Running
Null	Null				Kernel Driver	Running
nvdimm	Microsoft NVDIMM device driver	nvdimm.sys		10.0.19041.1	Kernel Driver	Stopped
nvraid	nvraid	nvraid.sys		10.6.0.23	Kernel Driver	Stopped
nvstor	nvstor	nvstor.sys		10.6.0.23	Kernel Driver	Stopped
Parport	Parallel port driver	parport.sys		10.0.19041.1	Kernel Driver	Running
partmgr	Partition driver	partmgr.sys		10.0.19041.1	Kernel Driver	Running
pci	PCI Bus Driver	pci.sys		10.0.19041.488	Kernel Driver	Running
pciide	pciide	pciide.sys		10.0.19041.488	Kernel Driver	Stopped
pcmcia	pcmcia	pcmcia.sys		10.0.19041.1	Kernel Driver	Stopped
pcw	Performance Counters for Windows Driver	pcw.sys		10.0.19041.1	Kernel Driver	Running
pdc	pdc	pdc.sys		10.0.19041.488	Kernel Driver	Running
PEAUTH	PEAUTH	peauth.sys		10.0.19041.488	Kernel Driver	Running
percsas2i	percsas2i	percsas2i.sys		6.805.3.0	Kernel Driver	Stopped
percsas3i	percsas3i	percsas3i.sys		6.604.6.0	Kernel Driver	Stopped
PktMon	Packet Monitor Driver	PktMon.sys		10.0.19041.1	Kernel Driver	Stopped
pmem	Microsoft persistent memory disk driver	pmem.sys		10.0.19041.1	Kernel Driver	Stopped
PNPMEM	Microsoft Memory Module Driver	pnpmem.sys		10.0.19041.1	Kernel Driver	Stopped
portcfg	portcfg	portcfg.sys		10.0.19041.1	Kernel Driver	Stopped
PptpMiniport	WAN Miniport (PPTP)	raspptp.sys		10.0.19041.488	Kernel Driver	Running
Processor	Processor Driver	processr.sys		10.0.19041.1	Kernel Driver	Stopped
Psched	QoS Packet Scheduler	pacer.sys		10.0.19041.1	Kernel Driver	Running
QWAVEdrv	QWAVE driver	qwavedrv.sys		10.0.19041.1	Kernel Driver	Running

Ramdisk	Windows RAM Disk Driver	ramdisk.sys	Navigation	1.1	Kernel Driver	Stopped
RasAcd	Remote Access Auto Connection Driver	rasacd.sys		10.0.19041.1	Kernel Driver	Stopped
RasAgileVpn	WAN Miniport (IKEv2)	AgileVpn.sys		10.0.19041.488	Kernel Driver	Running
Rasl2tp	WAN Miniport (L2TP)	rasl2tp.sys		10.0.19041.488	Kernel Driver	Running
RasPppoe	Remote Access PPPOE Driver	raspppoe.sys		10.0.19041.1	Kernel Driver	Running
RasSstp	WAN Miniport (SSTP)	rassstp.sys		10.0.19041.488	Kernel Driver	Running
rdbss	Redirected Buffering Sub System	rdbss.sys		10.0.19041.488	File System Driver	Running
rdpbus	Remote Desktop Device Redirector Bus Driver	rdpbus.sys		10.0.19041.1	Kernel Driver	Running
RDPDR	Remote Desktop Device Redirector Driver	rdpdr.sys		10.0.19041.1	Kernel Driver	Stopped
RdpVideoMiniport	Remote Desktop Video Miniport Driver	rdpvideominiport.sys		10.0.19041.153	Kernel Driver	Running
rdyboost	ReadyBoost	rdyboost.sys		10.0.19041.1	Kernel Driver	Running
ReFS	ReFS				File System Driver	Stopped
ReFSv1	ReFSv1				File System Driver	Stopped
RFCOMM	Bluetooth Device (RFCOMM Protocol TDI)	rfcomm.sys		10.0.19041.1	Kernel Driver	Stopped
rhproxy	Resource Hub proxy driver	rhproxy.sys		10.0.19041.1	Kernel Driver	Stopped
rspndr	Link-Layer Topology Discovery Responder	rspndr.sys		10.0.19041.1	Kernel Driver	Running
rt640x64	Realtek RT640 NT Driver	rt640x64.sys		10.42.526.2020	Kernel Driver	Running
s3cap	s3cap	vms3cap.sys		10.0.19041.1	Kernel Driver	Stopped
sbp2port	SBP-2 Transport/Protocol Bus Driver	sbp2port.sys		10.0.19041.1	Kernel Driver	Stopped
scfilter	Smart card PnP Class Filter Driver	scfilter.sys		10.0.19041.423	Kernel Driver	Stopped
scmbus	Microsoft Storage Class Memory Bus Driver	scmbus.sys		10.0.19041.1	Kernel Driver	Stopped
sdbus	sdbus	sdbus.sys		10.0.19041.488	Kernel Driver	Stopped
SDFRd	SDF Reflector	SDFRd.sys		10.0.19041.1	Kernel Driver	Stopped
sdstor	SD Storage Port Driver	sdstor.sys		10.0.19041.1	Kernel Driver	Stopped
SerCx	Serial UART Support Library	SerCx.sys		10.0.19041.1	Kernel Driver	Stopped
SerCx2	Serial UART Support Library	SerCx2.sys		10.0.19041.1	Kernel Driver	Stopped
Serenum	Serenum Filter Driver	serenum.sys		10.0.19041.1	Kernel Driver	Running
Serial	Serial port driver	serial.sys		10.0.19041.1	Kernel Driver	Running
sermouse	Serial Mouse Driver	sermouse.sys		10.0.19041.1	Kernel Driver	Stopped
sfloppy	High-Capacity Floppy Disk Drive	sfloppy.sys		10.0.19041.1	Kernel Driver	Stopped
SgrmAgent	System Guard Runtime Monitor Agent	SgrmAgent.sys		10.0.19041.1	Kernel Driver	Running
SiSRaid2	SiSRaid2	SiSRaid2.sys		5.1.1039.2600	Kernel Driver	Stopped
SiSRaid4	SiSRaid4	sisraid4.sys		5.1.1039.3600	Kernel Driver	Stopped
SmartSAMD	SmartSAMD	SmartSAMD.sys		1.50.1.0	Kernel Driver	Stopped
smbdirect	smbdirect	smbdirect.sys		10.0.19041.1	File System Driver	Stopped
spacedeskKtmInputMouse	spacedeskKtmInputMouse Service	spacedeskKtmInputMouse.sys			Kernel Driver	Stopped
spaceparser	Space Parser	spaceparser.sys		10.0.19041.1	Kernel Driver	Stopped
spaceport	Storage Spaces Driver	spaceport.sys		10.0.19041.423	Kernel Driver	Running
SpatialGraphFilter	Holographic Spatial Graph Filter	SpatialGraphFilter.sys		10.0.19041.1	Kernel Driver	Stopped
SpbCx	Simple Peripheral Bus Support Library	SpbCx.sys		10.0.19041.1	Kernel Driver	Stopped
srv2	Server SMB 2.xxx Driver	srv2.sys		10.0.19041.153	File System Driver	Running
srvnet	srvnet	srvnet.sys		10.0.19041.329	File System Driver	Running
ss_conn_usb_driver	SAMSUNG Mobile USB Connectivity Device Driver	ss_conn_usb_driver.sys		2.16.15.0	Kernel Driver	Stopped
ss_conn_usb_driver2	SAMSUNG Mobile USB Connectivity Device Driver V2	ss_conn_usb_driver2.sys		2.16.15.0	Kernel Driver	Stopped
ssuddmgr	SAMSUNG Mobile USB Device Management Serial Port(DEVGURU Ver.)	ssuddmgr.sys		2.16.15.0	Kernel Driver	Stopped
ssudmdm	SAMSUNG Mobile USB Modem Drivers (DEVGURU Ver.)	ssudmdm.sys		2.16.15.0	Kernel Driver	Running
ssudncm	SAMSUNG Mobile USB NCM Function Drivers	ssudncm.sys		2.16.15.0	Kernel Driver	Stopped
ssudobex	SAMSUNG Mobile USB OBEX Serial Port(DEVGURU Ver.)	ssudobex.sys		2.16.15.0	Kernel Driver	Stopped
ssudqcfilter	SAMSUNG Mobile USB QCRMNET Filter Driver	ssudqcfilter.sys		1.0.2.5	Kernel Driver	Stopped
ssudrmnet	SAMSUNG Mobile USB RMNET Drivers	ssudrmnet.sys		2.16.15.0	Kernel Driver	Stopped
ssudserd	SAMSUNG Mobile USB Diagnostic Serial Port(DEVGURU Ver.)	ssudserd.sys		2.16.15.0	Kernel Driver	Stopped
stexstor	stexstor	stexstor.sys		5.1.0.10	Kernel Driver	Stopped
storahci	Microsoft Standard SATA AHCI Driver	storahci.sys		10.0.19041.488	Kernel Driver	Running
storflt	Microsoft Hyper-V Storage Accelerator	vmstorfl.sys		10.0.19041.1	Kernel Driver	Stopped
stornvme	Microsoft Standard NVM Express Driver	stornvme.sys		10.0.19041.488	Kernel Driver	Stopped

storqosflt	Storage QoS Filter Driver	storqosflt.sys	Navigation	1.1	File System Driver	Running
storufs	Microsoft Universal Flash Storage (UFS) Driver	storufs.sys		10.0.19041.488	Kernel Driver	Stopped
storvsc	storvsc	storvsc.sys		10.0.19041.1	Kernel Driver	Stopped
swenum	Software Bus Driver	swenum.sys		10.0.19041.1	Kernel Driver	Running
Synth3dVsc	Synth3dVsc	Synth3dVsc.sys		10.0.19041.1	Kernel Driver	Stopped
Tcpip	TCP/IP Protocol Driver	tcpip.sys		10.0.19041.488	Kernel Driver	Running
Tcpip6	@todo.dll,-100;Microsoft IPv6 Protocol Driver	tcpip.sys		10.0.19041.488	Kernel Driver	Stopped
tcpipreg	TCP/IP Registry Compatibility	tcpipreg.sys		10.0.19041.1	Kernel Driver	Running
tdx	NetIO Legacy TDI Support Driver	tdx.sys		10.0.19041.1	Kernel Driver	Running
Telemetry	Intel(R) Telemetry Service	IntelTA.sys		10.0.19041.423	Kernel Driver	Running
terminpt	Microsoft Remote Desktop Input Driver	terminpt.sys		10.0.19041.1	Kernel Driver	Stopped
TPM	TPM	tpm.sys		10.0.19041.488	Kernel Driver	Stopped
TsUsbFlt	Remote Desktop USB Hub Class Filter Driver	tsusbflt.sys		10.0.19041.1	Kernel Driver	Stopped
TsUsbGD	Remote Desktop Generic USB Device	TsUsbGD.sys		10.0.19041.1	Kernel Driver	Stopped
tsusbhub	Remote Desktop USB Hub	tsusbhub.sys		10.0.19041.153	Kernel Driver	Stopped
tunnel	Microsoft Tunnel Miniport Adapter Driver	tunnel.sys		10.0.19041.1	Kernel Driver	Stopped
UASPStor	USB Attached SCSI (UAS) Driver	uaspstor.sys		10.0.19041.1	Kernel Driver	Stopped
UcmCx0101	USB Connector Manager KMDF Class Extension	UcmCx.sys		10.0.19041.1	Kernel Driver	Stopped
UcmTcpciCx0101	UCM-TCPCI KMDF Class Extension	UcmTcpciCx.sys		10.0.19041.1	Kernel Driver	Stopped
UcmUcsiAcpiClient	UCM-UCSI ACPI Client	UcmUcsiAcpiClient.sys		10.0.19041.1	Kernel Driver	Stopped
UcmUcsiCx0101	UCM-UCSI KMDF Class Extension	UcmUcsiCx.sys		10.0.19041.488	Kernel Driver	Stopped
Ucx01000	USB Host Support Library	ucx01000.sys		10.0.19041.1	Kernel Driver	Running
UdeCx	USB Device Emulation Support Library	udecx.sys		10.0.19041.1	Kernel Driver	Stopped
udfs	udfs	udfs.sys		10.0.19041.1	File System Driver	Stopped
UEFI	Microsoft UEFI Driver	UEFI.sys		10.0.19041.1	Kernel Driver	Stopped
UevAgentDriver	UevAgentDriver	UevAgentDriver.sys		10.0.19041.1	File System Driver	Stopped
Ufx01000	USB Function Class Extension	ufx01000.sys		10.0.19041.1	Kernel Driver	Stopped
UfxChipidea	USB Chipidea Controller	UfxChipidea.sys		10.0.19041.1	Kernel Driver	Stopped
ufxsynopsys	USB Synopsys Controller	ufxsynopsys.sys		10.0.19041.1	Kernel Driver	Stopped
umbus	UMBus Enumerator Driver	umbus.sys		10.0.19041.1	Kernel Driver	Running
UmPass	Microsoft UMPass Driver	umpass.sys		10.0.19041.1	Kernel Driver	Stopped
UrsChipidea	Chipidea USB Role-Switch Driver	urschipidea.sys		10.0.19041.1	Kernel Driver	Stopped
UrsCx01000	USB Role-Switch Support Library	urscx01000.sys		10.0.19041.1	Kernel Driver	Stopped
UrsSynopsys	Synopsys USB Role-Switch Driver	urssynopsys.sys		10.0.19041.1	Kernel Driver	Stopped
usbaudio	USB Audio Driver (WDM)	usbaudio.sys		10.0.19041.388	Kernel Driver	Stopped
usbaudio2	USB Audio 2.0 Service	usbaudio2.sys		10.0.19041.1	Kernel Driver	Stopped
usbccgp	Microsoft USB Generic Parent Driver	usbccgp.sys		10.0.19041.488	Kernel Driver	Running
usbcir	eHome Infrared Receiver (USBCIR)	usbcir.sys		10.0.19041.1	Kernel Driver	Stopped
usbehci	Microsoft USB 2.0 Enhanced Host Controller Miniport Driver	usbehci.sys		10.0.19041.1	Kernel Driver	Running
usbhub	Microsoft USB Standard Hub Driver	usbhub.sys		10.0.19041.1	Kernel Driver	Running
USBHUB3	SuperSpeed Hub	UsbHub3.sys		10.0.19041.264	Kernel Driver	Running
usbohci	Microsoft USB Open Host Controller Miniport Driver	usbohci.sys		10.0.19041.1	Kernel Driver	Stopped
usbprint	Microsoft USB PRINTER Class	usbprint.sys		10.0.19041.1	Kernel Driver	Stopped
usbser	Microsoft USB Serial Driver	usbser.sys		10.0.19041.1	Kernel Driver	Stopped
USBSTOR	USB Mass Storage Driver	USBSTOR.SYS		10.0.19041.1	Kernel Driver	Stopped
usbuhci	Microsoft USB Universal Host Controller Miniport Driver	usbuhci.sys		10.0.19041.1	Kernel Driver	Stopped
USBXHCI	USB xHCI Compliant Host Controller	USBXHCI.SYS		10.0.19041.488	Kernel Driver	Running
vdrvroot	Microsoft Virtual Drive Enumerator	vdrvroot.sys		10.0.19041.1	Kernel Driver	Running
VerifierExt	Driver Verifier Extension	VerifierExt.sys		10.0.19041.1	Kernel Driver	Stopped
vhdmp	vhdmp	vhdmp.sys		10.0.19041.84	Kernel Driver	Stopped
vhf	Virtual HID Framework (VHF) Driver	vhf.sys		10.0.19041.1	Kernel Driver	Stopped
Vid	Vid	Vid.sys		10.0.19041.423	Kernel Driver	Running
VirtualRender	VirtualRender	vrd.sys		10.0.19041.1	Kernel Driver	Stopped
vmbus	Virtual Machine Bus	vmbus.sys		10.0.19041.488	Kernel Driver	Stopped
VMBusHID	VMBusHID	VMBusHID.sys		10.0.19041.1	Kernel Driver	Stopped

vmgid	Microsoft Hyper-V Guest Infrastructure Driver	vmgid.sys	Navigation	1.1	Kernel Driver	Stopped
volmgr	Volume Manager Driver	volmgr.sys		10.0.19041.1	Kernel Driver	Running
volmgrx	Dynamic Volume Manager	volmgrx.sys		10.0.19041.1	Kernel Driver	Running
volsnap	Volume Shadow Copy driver	volsnap.sys		10.0.19041.488	Kernel Driver	Running
volume	Volume driver	volume.sys		10.0.19041.1	Kernel Driver	Running
vpci	Microsoft Hyper-V Virtual PCI Bus	vpci.sys		10.0.19041.1	Kernel Driver	Stopped
vsmraid	vsmraid	vsmraid.sys		7.0.9600.6352	Kernel Driver	Stopped
VSTXRAID	VIA StorX Storage RAID Controller Windows Driver	vstxraid.sys		8.0.9200.8110	Kernel Driver	Stopped
vwifibus	Virtual Wireless Bus Driver	vwifibus.sys		10.0.19041.1	Kernel Driver	Stopped
vwififlt	Virtual WiFi Filter Driver	vwififlt.sys		10.0.19041.1	Kernel Driver	Running
WacomPen	Wacom Serial Pen HID Driver	wacompen.sys		10.0.19041.1	Kernel Driver	Stopped
wanarp	Remote Access IP ARP Driver	wanarp.sys		10.0.19041.1	Kernel Driver	Running
wanarpv6	Remote Access IPv6 ARP Driver	wanarp.sys		10.0.19041.1	Kernel Driver	Stopped
wcifs	Windows Container Isolation	wcifs.sys		10.0.19041.1	File System Driver	Running
wcnfs	Windows Container Name Virtualization	wcnfs.sys		10.0.19041.1	File System Driver	Stopped
WdBoot	Microsoft Defender Antivirus Boot Driver	WdBoot.sys		4.18.2008.9	Kernel Driver	Stopped
Wdf01000	Kernel Mode Driver Frameworks service	Wdf01000.sys		1.31.19041.423	Kernel Driver	Running
WdFilter	Microsoft Defender Antivirus Mini-Filter Driver	WdFilter.sys		4.18.2008.9	File System Driver	Running
wdiwifi	WDI Driver Framework	wdiwifi.sys		10.0.19041.488	Kernel Driver	Stopped
WdmCompanionFilter	WdmCompanionFilter	WdmCompanionFilter.sys		10.0.19041.1	Kernel Driver	Stopped
WdNisDrv	Microsoft Defender Antivirus Network Inspection System Driver	WdNisDrv.sys		4.18.2008.9	Kernel Driver	Running
WFPLWFS	Microsoft Windows Filtering Platform	wfplwfs.sys		10.0.19041.488	Kernel Driver	Running
WIMMount	WIMMount	wimmount.sys		10.0.19041.423	File System Driver	Stopped
WindowsTrustedRT	Windows Trusted Execution Environment Class Extension	WindowsTrustedRT.sys		10.0.19041.1	Kernel Driver	Running
WindowsTrustedRTProxy	Microsoft Windows Trusted Runtime Secure Service	WindowsTrustedRTProxy.sys		10.0.19041.1	Kernel Driver	Running
WinMad	WinMad Service	winmad.sys		5.50.14695.0	Kernel Driver	Stopped
WinNat	Windows NAT Driver	winnat.sys		10.0.19041.488	Kernel Driver	Stopped
WINUSB	Generic driver for USB devices	WinUSB.sys		10.0.19041.1	Kernel Driver	Running
WinVerbs	WinVerbs Service	winverbs.sys		5.50.14695.0	Kernel Driver	Stopped
WmiAcpi	Microsoft Windows Management Interface for ACPI	wmiacpi.sys		10.0.19041.1	Kernel Driver	Stopped
Wof	Windows Overlay File System Filter Driver				File System Driver	Running
wovad_micarray	WO Mic Device	womic.sys		10.0.10011.16384	Kernel Driver	Running
WpdUpFltr	WPD Upper Class Filter Driver	WpdUpFltr.sys		10.0.19041.1	Kernel Driver	Running
ws2ifsl	Winsock IFS Driver	ws2ifsl.sys		10.0.19041.1	Kernel Driver	Stopped
WudfPf	User Mode Driver Frameworks Platform Driver	WudfPf.sys		10.0.19041.1	Kernel Driver	Stopped
WUDFRd	Windows Driver Foundation - User-mode Driver Framework Reflector	WUDFRd.sys		10.0.19041.1	Kernel Driver	Running
WUDFWpdFs	WPD File System driver	WUDFRd.sys		10.0.19041.1	Kernel Driver	Running
WUDFWpdMtp	WUDFWpdMtp	WUDFRd.sys		10.0.19041.1	Kernel Driver	Running
xboxgip	Xbox Game Input Protocol Driver	xboxgip.sys		10.0.19041.1	Kernel Driver	Stopped
xinputhid	XINPUT HID Filter Driver	xinputhid.sys		10.0.19041.1	Kernel Driver	Stopped
Xvdd	XVDD Port Driver	xvdd.sys		10.0.19041.3952	Kernel Driver	Stopped

Services

Service Name	Service Description	File Name	Version	Type	State	Account
AarSvc_eba974	Agent Activation Runtime_eba974	svchost.exe	10.0.19041.1	Unknown	Running	
AdAppMgrSvc	Autodesk Desktop App Service	AdAppMgrSvc.exe	8.0.0.46	Own Process	Running	LocalSystem
AdskLicensingService	Autodesk Desktop Licensing Service	AdskLicensingService.exe	10.11.1.1760	Own Process	Running	NT Authority\LocalService
AJRouter	AllJoyn Router Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
ALG	Application Layer Gateway Service	alg.exe	10.0.19041.1	Own	Stopped	NT

Navigation

				Process		AUTHORITY\LocalService
AppIDSvc	Application Identity	svchost.exe	10.0.19041.1	Process	Stopped	NT Authority\LocalService
Appinfo	Application Information	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
AppMgmt	Application Management	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
AppReadiness	App Readiness	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
AppVClient	Microsoft App-V Client	AppVClient.exe	10.0.19041.84	Own Process	Stopped	LocalSystem
AppXSvc	AppX Deployment Service (AppXSVC)	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
AssignedAccessManagerSvc	AssignedAccessManager Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
AudioEndpointBuilder	Windows Audio Endpoint Builder	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
Audiosrv	Windows Audio	svchost.exe	10.0.19041.1	Own Process	Running	NT AUTHORITY\LocalService
autotimesvc	Cellular Time	svchost.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\LocalService
AxInstSV	ActiveX Installer (AxInstSV)	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
BcastDVRUserService_eba974	GameDVR and Broadcast User Service_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
BDESVC	BitLocker Drive Encryption Service	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
BFE	Base Filtering Engine	svchost.exe	10.0.19041.1	Share Process	Running	NT AUTHORITY\LocalService
BITS	Background Intelligent Transfer Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
BluetoothUserService_eba974	Bluetooth User Support Service_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
BrokerInfrastructure	Background Tasks Infrastructure Service	svchost.exe	10.0.19041.1	Share Process	Running	LocalSystem
BTAGService	Bluetooth Audio Gateway Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
BthAvctpSvc	AVCTP service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
bthserv	Bluetooth Support Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
BtSwitcherService	CSR Bluetooth Switcher Service	BtSwitcherService.exe	2.1.63.0	Own Process	Running	LocalSystem
camsvc	Capability Access Manager Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
CaptureService_eba974	CaptureService_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
cbdhsvc_eba974	Clipboard User Service_eba974	svchost.exe	10.0.19041.1	Unknown	Running	
CDPSvc	Connected Devices Platform Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
CDPUserSvc_eba974	Connected Devices Platform User Service_eba974	svchost.exe	10.0.19041.1	Unknown	Running	
CertPropSvc	Certificate Propagation	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
chromoting	Chrome Remote Desktop Service	remoting_host.exe	85.0.4183.6	Own Process	Running	LocalSystem
ClickToRunSvc	Microsoft Office Click-to-Run Service	OfficeClickToRun.exe	16.0.12527.20986	Own Process	Running	LocalSystem
ClipSVC	Client License Service (ClipSVC)	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
COMSysApp	COM+ System Application	dllhost.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
ConsentUxUserSvc_eba974	ConsentUX_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
CoreMessagingRegistrar	CoreMessaging	svchost.exe	10.0.19041.1	Share Process	Running	NT AUTHORITY\LocalService
cphs	Intel(R) Content Protection HECI Service	IntelCpHeciSvc.exe	9.0.1.1117	Own Process	Stopped	LocalSystem
CredentialEnrollmentManagerUserSvc_eba974	CredentialEnrollmentManagerUserSvc_eba974	CredentialEnrollmentManager.exe	10.0.19041.388	Unknown	Stopped	

CryptSvc	Cryptographic Services	svchost.exe	10.0 Navigation	wn	Running	NT Authority\NetworkService
CscService	Offline Files	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
CSRBtAudioService	CSR Bluetooth Audio Service	CsrBtAudioService.exe	2.1.63.0	Own Process	Running	LocalSystem
CsrBtOBEXService	CSR OBEX Service	CsrBtOBEXService.exe	2.1.63.0	Own Process	Running	LocalSystem
CsrBtService	CSR Bluetooth Service	CsrBtService.exe	2.1.63.0	Own Process	Running	LocalSystem
DcomLaunch	DCOM Server Process Launcher	svchost.exe	10.0.19041.1	Share Process	Running	LocalSystem
debugregsvc	debugregsvc	svchost.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
defragsvc	Optimize drives	svchost.exe	10.0.19041.1	Own Process	Stopped	localSystem
DeveloperToolsService	Developer Tools Service	DeveloperToolsSvc.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
DeviceAssociationBrokerSvc_eba974	DeviceAssociationBroker_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
DeviceAssociationService	Device Association Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
DeviceInstall	Device Install Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
DevicePickerUserSvc_eba974	DevicePicker_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
DevicesFlowUserSvc_eba974	DevicesFlow_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
DevQueryBroker	DevQuery Background Discovery Broker	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
Dhcp	DHCP Client	svchost.exe	10.0.19041.1	Unknown	Running	NT Authority\LocalService
diagnosticshub.standardcollector.service	Microsoft (R) Diagnostics Hub Standard Collector Service	DiagnosticsHub.StandardCollector.Service.exe	11.0.19041.508	Own Process	Stopped	LocalSystem
diagsvc	Diagnostic Execution Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
DiagTrack	Connected User Experiences and Telemetry	svchost.exe	10.0.19041.1	Own Process	Running	LocalSystem
DispBrokerDesktopSvc	Display Policy Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
DisplayEnhancementService	Display Enhancement Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
DmEnrollmentSvc	Device Management Enrollment Service	svchost.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
dmwappushservice	Device Management Wireless Application Protocol (WAP) Push message Routing Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
Dnscache	DNS Client	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\NetworkService
DoSvc	Delivery Optimization	svchost.exe	10.0.19041.1	Unknown	Running	NT Authority\NetworkService
dot3svc	Wired AutoConfig	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
DPS	Diagnostic Policy Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
DsmSvc	Device Setup Manager	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
DsSvc	Data Sharing Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
DusmSvc	Data Usage	svchost.exe	10.0.19041.1	Own Process	Running	NT Authority\LocalService
Eaphost	Extensible Authentication Protocol	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
edgeupdate	Microsoft Edge Update Service (edgeupdate)	MicrosoftEdgeUpdate.exe	1.3.133.5	Own Process	Stopped	LocalSystem
edgeupdatem	Microsoft Edge Update Service (edgeupdatem)	MicrosoftEdgeUpdate.exe	1.3.133.5	Own Process	Stopped	LocalSystem
EFS	Encrypting File System (EFS)	lsass.exe	10.0.19041.488	Share	Running	LocalSystem

Navigation

embeddedmode	Embedded Mode	svchost.exe	10.0.19041.1	Process	Stopped	LocalSystem
EntAppSvc	Enterprise App Management Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
EventLog	Windows Event Log	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
EventSystem	COM+ Event System	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
Fax	Fax	fxssvc.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\NetworkService
fdPHost	Function Discovery Provider Host	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
FDResPub	Function Discovery Resource Publication	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
fhsvc	File History Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
FlexNet Licensing Service	FlexNet Licensing Service	FNPLicensingService.exe	11.16.0.0	Own Process	Running	LocalSystem
FontCache	Windows Font Cache Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
FontCache3.0.0.0	Windows Presentation Foundation Font Cache 3.0.0.0	PresentationFontCache.exe	3.0.6920.9141	Own Process	Running	NT Authority\LocalService
FrameServer	Windows Camera Frame Server	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
Fuj02e3DriverUtilityService	Fujitsu FUJ02E3 Device Driver - Utility Service	fuj02e3-utility.exe	4.3.0.0	Own Process	Running	LocalSystem
gpsvc	Group Policy Client	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
GraphicsPerfSvc	GraphicsPerfSvc	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
hidserv	Human Interface Device Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
HvHost	HV Host Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
icssvc	Windows Mobile Hotspot Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT Authority\LocalService
igfxCUIService1.0.0.0	Intel(R) HD Graphics Control Panel Service	igfxCUIService.exe	6.15.10.5129	Own Process	Running	LocalSystem
IKEEXT	IKE and AuthIP IPsec Keying Modules	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
InstallService	Microsoft Store Install Service	svchost.exe	10.0.19041.1	Own Process	Running	LocalSystem
iphlpsvc	IP Helper	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
IpxlatCfgSvc	IP Translation Configuration Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
KeyIso	CNG Key Isolation	lsass.exe	10.0.19041.488	Share Process	Running	LocalSystem
KtmRm	KtmRm for Distributed Transaction Coordinator	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\NetworkService
LanmanServer	Server	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
LanmanWorkstation	Workstation	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\NetworkService
lfsvc	Geolocation Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
LicenseManager	Windows License Manager Service	svchost.exe	10.0.19041.1	Unknown	Running	NT Authority\LocalService
lltdsvc	Link-Layer Topology Discovery Mapper	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
lmhosts	TCP/IP NetBIOS Helper	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
LSM	Local Session Manager	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
LxpSvc	Language Experience Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem

MapsBroker	Downloaded Maps Manager	svchost.exe	10.0	Navigation	Stopped	NT AUTHORITY\NetworkService
MessagingService_eba974	MessagingService_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)	elevation_service.exe	85.0.564.51	Own Process	Stopped	LocalSystem
MixedRealityOpenXRSvc	Windows Mixed Reality OpenXR Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
mpssvc	Windows Defender Firewall	svchost.exe	10.0.19041.1	Share Process	Running	NT Authority\LocalService
MSDTC	Distributed Transaction Coordinator	msdtc.exe	2001.12.10941.16384	Own Process	Stopped	NT AUTHORITY\NetworkService
MSiSCSI	Microsoft iSCSI Initiator Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
msiserver	Windows Installer	msiexec.exe	5.0.19041.1	Own Process	Stopped	LocalSystem
NaturalAuthentication	Natural Authentication	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
NcaSvc	Network Connectivity Assistant	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
NcbService	Network Connection Broker	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
NcdAutoSetup	Network Connected Devices Auto-Setup	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
Netlogon	Netlogon	lsass.exe	10.0.19041.488	Share Process	Stopped	LocalSystem
Netman	Network Connections	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
netprofm	Network List Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
NetSetupSvc	Network Setup Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
NetTcpPortSharing	Net.Tcp Port Sharing Service	SMSvcHost.exe	4.8.4084.0	Share Process	Stopped	NT AUTHORITY\LocalService
NgcCtnrSvc	Microsoft Passport Container	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
NgcSvc	Microsoft Passport	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
NlaSvc	Network Location Awareness	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\NetworkService
nsi	Network Store Interface Service	svchost.exe	10.0.19041.1	Unknown	Running	NT Authority\LocalService
OneSyncSvc_eba974	Sync Host_eba974	svchost.exe	10.0.19041.1	Unknown	Running	
ose	Office Source Engine	OSE.EXE	16.0.12527.20988	Own Process	Stopped	LocalSystem
p2pimsvc	Peer Networking Identity Manager	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
p2psvc	Peer Networking Grouping	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
PcaSvc	Program Compatibility Assistant Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
PeerDistSvc	BranchCache	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\NetworkService
perceptionsimulation	Windows Perception Simulation Service	PerceptionSimulationService.exe	10.0.19041.84	Own Process	Stopped	LocalSystem
PerfHost	Performance Counter DLL Host	perfhost.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\LocalService
PhoneSvc	Phone Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT Authority\LocalService
PimIndexMaintenanceSvc_eba974	Contact Data_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
pla	Performance Logs & Alerts	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
PlugPlay	Plug and Play	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
PNRPAutoReg	PNRP Machine Name Publication Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService

PNRPsvc	Peer Name Resolution Protocol	svchost.exe	10.0	Navigation	Stopped	NT AUTHORITY\LocalService
PolicyAgent	IPsec Policy Agent	svchost.exe	10.0.19041.1	Unknown	Running	NT Authority\NetworkService
Power	Power	svchost.exe	10.0.19041.1	Share Process	Running	LocalSystem
PrintNotify	Printer Extensions and Notifications	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
PrintWorkflowUserSvc_eba974	PrintWorkflow_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
ProfSvc	User Profile Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
PushToInstall	Windows PushToInstall Service	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
QWAVE	Quality Windows Audio Video Experience	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
RasAuto	Remote Access Auto Connection Manager	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
RasMan	Remote Access Connection Manager	svchost.exe	10.0.19041.1	Share Process	Running	localSystem
RemoteAccess	Routing and Remote Access	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
RemoteRegistry	Remote Registry	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
RetailDemo	Retail Demo Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
RmSvc	Radio Management Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
RpcEptMapper	RPC Endpoint Mapper	svchost.exe	10.0.19041.1	Share Process	Running	NT AUTHORITY\NetworkService
RpcLocator	Remote Procedure Call (RPC) Locator	locator.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\NetworkService
RpcSs	Remote Procedure Call (RPC)	svchost.exe	10.0.19041.1	Share Process	Running	NT AUTHORITY\NetworkService
SamSs	Security Accounts Manager	lsass.exe	10.0.19041.488	Share Process	Running	LocalSystem
SCardSvr	Smart Card	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
ScDeviceEnum	Smart Card Device Enumeration Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
Schedule	Task Scheduler	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
SCPolicySvc	Smart Card Removal Policy	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
SDRSVC	Windows Backup	svchost.exe	10.0.19041.1	Own Process	Stopped	localSystem
seclogon	Secondary Logon	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
SecurityHealthService	Windows Security Service	SecurityHealthService.exe	4.18.1907.16384	Own Process	Running	LocalSystem
SEMgrSvc	Payments and NFC/SE Manager	svchost.exe	10.0.19041.1	Own Process	Running	NT AUTHORITY\LocalService
SENS	System Event Notification Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
Sense	Windows Defender Advanced Threat Protection Service	MsSense.exe		Own Process	Stopped	LocalSystem
SensorDataService	Sensor Data Service	SensorDataService.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
SensorService	Sensor Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
SensrSvc	Sensor Monitoring Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
SessionEnv	Remote Desktop Configuration	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
SgrmBroker	System Guard Runtime Monitor Broker	SgrmBroker.exe	10.0.19041.84	Own Process	Running	LocalSystem

SharedAccess	Internet Connection Sharing (ICS)	svchost.exe	10.0	Navigation	Stopped	LocalSystem
SharedRealitySvc	Spatial Data Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
ShellHWDetection	Shell Hardware Detection	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
shpamsvc	Shared PC Account Manager	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
smphost	Microsoft Storage Spaces SMP	svchost.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\NetworkService
SmsRouter	Microsoft Windows SMS Router Service.	svchost.exe	10.0.19041.1	Share Process	Stopped	NT Authority\LocalService
SNMPTRAP	SNMP Trap	snmptrap.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\LocalService
spectrum	Windows Perception Service	spectrum.exe	10.0.19041.153	Own Process	Stopped	NT AUTHORITY\LocalService
Spooler	Print Spooler	spoolsv.exe	10.0.19041.423	Own Process	Running	LocalSystem
sppsvc	Software Protection	sppsvc.exe	10.0.19041.508	Own Process	Running	NT AUTHORITY\NetworkService
ss_conn_launcher_service	SAMSUNG Mobile USB Connectivity Launcher	ss_conn_launcher.exe	2.16.15.0	Own Process	Stopped	LocalSystem
SSDPSRV	SSDP Discovery	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
ssh-agent	OpenSSH Authentication Agent	ssh-agent.exe	7.7.2.1	Own Process	Stopped	LocalSystem
sshd	OpenSSH SSH Server	sshd.exe	7.7.2.3	Own Process	Stopped	LocalSystem
SshdBroker	SshdBroker	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
SstpSvc	Secure Socket Tunneling Protocol Service	svchost.exe	10.0.19041.1	Unknown	Running	NT Authority\LocalService
StateRepository	State Repository Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
stisvc	Windows Image Acquisition (WIA)	svchost.exe	10.0.19041.1	Own Process	Running	NT Authority\LocalService
StorSvc	Storage Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
svsvc	Spot Verifier	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
swprv	Microsoft Software Shadow Copy Provider	svchost.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
SysMain	SysMain	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
SystemEventsBroker	System Events Broker	svchost.exe	10.0.19041.1	Share Process	Running	LocalSystem
TabletInputService	Touch Keyboard and Handwriting Panel Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
TapiSrv	Telephony	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\NetworkService
TermService	Remote Desktop Services	svchost.exe	10.0.19041.1	Share Process	Stopped	NT Authority\NetworkService
Themes	Themes	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
TieringEngineService	Storage Tiers Management	TieringEngineService.exe	10.0.19041.1	Own Process	Stopped	localSystem
TimeBrokerSvc	Time Broker	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
TokenBroker	Web Account Manager	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
TrkWks	Distributed Link Tracking Client	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
TroubleshootingSvc	Recommended Troubleshooting Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
TrustedInstaller	Windows Modules Installer	TrustedInstaller.exe	10.0.19041.329	Own Process	Stopped	localSystem
tzautoupdate	Auto Time Zone Updater	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService

UdkUserSvc_eba974	Udk User Service_eba974	svchost.exe	10.0	wn	Stopped	
UevAgentService	User Experience Virtualization Service	AgentService.exe	10.0.19041.488	Process	Stopped	LocalSystem
UmRdpService	Remote Desktop Services UserMode Port Redirector	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
UnistoreSvc_eba974	User Data Storage_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
upnphost	UPnP Device Host	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
UserDataSvc_eba974	User Data Access_eba974	svchost.exe	10.0.19041.1	Unknown	Stopped	
UserManager	User Manager	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
UsoSvc	Update Orchestrator Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
VacSvc	Volumetric Audio Compositor Service	svchost.exe	10.0.19041.1	Own Process	Stopped	NT AUTHORITY\LocalService
VaultSvc	Credential Manager	lsass.exe	10.0.19041.488	Share Process	Running	LocalSystem
vds	Virtual Disk	vds.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
vmicguestinterface	Hyper-V Guest Service Interface	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
vmicheartbeat	Hyper-V Heartbeat Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
vmickvpexchange	Hyper-V Data Exchange Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
vmicrdv	Hyper-V Remote Desktop Virtualization Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
vmicshutdown	Hyper-V Guest Shutdown Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
vmictimesync	Hyper-V Time Synchronization Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
vmicvmsession	Hyper-V PowerShell Direct Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
vmicvss	Hyper-V Volume Shadow Copy Requestor	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
VRLService	VRLService	vrol.exe	5.1.2.12916	Own Process	Running	LocalSystem
vrswrm-service	V-Ray Swarm	Program		Own Process	Running	LocalSystem
VSS	Volume Shadow Copy	vssvc.exe	10.0.19041.329	Own Process	Stopped	LocalSystem
W32Time	Windows Time	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
WaaSMedicSvc	Windows Update Medic Service	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
WalletService	WalletService	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
WarpJITSvc	WarpJITSvc	svchost.exe	10.0.19041.1	Own Process	Stopped	NT Authority\LocalService
wbengine	Block Level Backup Engine Service	wbengine.exe	10.0.19041.329	Own Process	Stopped	localSystem
WbioSrvc	Windows Biometric Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
Wcmsvc	Windows Connection Manager	svchost.exe	10.0.19041.1	Own Process	Running	NT Authority\LocalService
wcncsvc	Windows Connect Now - Config Registrar	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
WdiServiceHost	Diagnostic Service Host	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
WdiSystemHost	Diagnostic System Host	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
WdNisSvc	Microsoft Defender Antivirus Network Inspection Service	NisSrv.exe	4.18.2008.9	Own Process	Running	NT AUTHORITY\LocalService
WebClient	WebClient	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService

WebManagement	Web Management	WebManagement.exe	10.0	Navigation	Stopped	LocalSystem
Wecsvc	Windows Event Collector	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\NetworkService
WEPHOSTSVC	Windows Encryption Provider Host Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
wercplsupport	Problem Reports Control Panel Support	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
WerSvc	Windows Error Reporting Service	svchost.exe	10.0.19041.1	Own Process	Stopped	localSystem
WFDSConMgrSvc	Wi-Fi Direct Services Connection Manager Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
WiaRpc	Still Image Acquisition Events	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
WinDefend	Microsoft Defender Antivirus Service	MsMpEng.exe	4.18.2008.9	Own Process	Running	LocalSystem
WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
Winmgmt	Windows Management Instrumentation	svchost.exe	10.0.19041.1	Unknown	Running	localSystem
WinRM	Windows Remote Management (WS-Management)	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\NetworkService
wisvc	Windows Insider Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
WlanSvc	WLAN AutoConfig	svchost.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
wlidsvc	Microsoft Account Sign-in Assistant	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
wlpasvc	Local Profile Assistant Service	svchost.exe	10.0.19041.1	Share Process	Stopped	NT Authority\LocalService
WManSvc	Windows Management Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
wmiApSrv	WMI Performance Adapter	WmiApSrv.exe	10.0.19041.1	Own Process	Stopped	localSystem
workfolderssvc	Work Folders	svchost.exe	10.0.19041.1	Share Process	Stopped	NT AUTHORITY\LocalService
WpcMonSvc	Parental Controls	svchost.exe	10.0.19041.1	Own Process	Stopped	LocalSystem
WPDBusEnum	Portable Device Enumerator Service	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
WpnService	Windows Push Notifications System Service	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
WpnUserService_eba974	Windows Push Notifications User Service_eba974	svchost.exe	10.0.19041.1	Unknown	Running	
wscsvc	Security Center	svchost.exe	10.0.19041.1	Unknown	Running	NT AUTHORITY\LocalService
WSearch	Windows Search	SearchIndexer.exe	7.0.19041.488	Own Process	Running	LocalSystem
wuauserv	Windows Update	svchost.exe	10.0.19041.1	Unknown	Running	LocalSystem
WwanSvc	WWAN AutoConfig	svchost.exe	10.0.19041.1	Share Process	Stopped	localSystem
XblAuthManager	Xbox Live Auth Manager	svchost.exe	10.0.19041.1	Unknown	Stopped	LocalSystem
XblGameSave	Xbox Live Game Save	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
XboxGipSvc	Xbox Accessory Management Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem
XboxNetApiSvc	Xbox Live Networking Service	svchost.exe	10.0.19041.1	Share Process	Stopped	LocalSystem

AX Files

AX File	Version	Description
bdaplgin.ax	10.0.19041.1	Microsoft BDA Device Control Plug-in for MPEG2 based networks.
g711codc.ax	10.0.19041.1	Intel G711 CODEC
iac25_32.ax	2.0.5.53	Indeo® audio software
ir41_32.ax	10.0.19041.1	IR41_32 WRAPPER DLL
ivfsrc.ax	5.10.2.51	Intel Indeo® video IVF Source Filter 5.10
ksproxy.ax	10.0.19041.1	WDM Streaming ActiveMovie Proxy
kstvtune.ax	10.0.19041.1	WDM Streaming TvTuner
kswdmcap.ax	10.0.19041.1	WDM Streaming Video Capture
ksxbar.ax	10.0.19041.1	WDM Streaming Crossbar
mpeg2data.ax	10.0.19041.1	Microsoft MPEG-2 Section and Table Acquisition Module
mpg2splt.ax	10.0.19041.329	DirectShow MPEG-2 Splitter.
msdvbnp.ax	10.0.19041.1	Microsoft Network Provider for MPEG2 based networks.
msnp.ax	10.0.19041.1	Microsoft Network Provider for MPEG2 based networks.
psisrndr.ax	10.0.19041.1	Microsoft Transport Information Filter for MPEG2 based networks.
vbicodec.ax	10.0.19041.1	Microsoft VBI Codec
vbisurf.ax	10.0.19041.1	VBI Surface Allocator Filter
vidcap.ax	10.0.19041.1	Video Capture Interface Server
wstpager.ax	10.0.19041.1	Microsoft Teletext Server

Navigation

DLL Files

DLL File	Version	Description
aadauthhelper.dll	10.0.19041.1	Microsoft® AAD Auth Helper
aadtb.dll	10.0.19041.117	AAD Token Broker Helper Library
aadwamextension.dll	10.0.19041.488	AAD WAM extension DLL
aarsvc.dll	10.0.19041.423	Agent Activation Runtime Service
abovelockapphost.dll	10.0.19041.388	AboveLockAppHost
accessibilitycpl.dll	10.0.19041.423	Ease of access control panel
accountaccessor.dll	10.0.19041.1	Sync data model to access accounts
accountsrt.dll	10.0.19041.264	Accounts RT utilities for mail, contacts, calendar
acgenral.dll	10.0.19041.1	Windows Compatibility DLL
aclayers.dll	10.0.19041.1	Windows Compatibility DLL
acledit.dll	10.0.19041.1	Access Control List Editor
aclui.dll	10.0.19041.1	Security Descriptor Editor
acppage.dll	10.0.19041.1	Compatibility Tab Shell Extension Library
acspecfc.dll	10.0.19041.423	Windows Compatibility DLL
actioncenter.dll	10.0.19041.1	Security and Maintenance
actioncentercpl.dll	10.0.19041.423	Security and Maintenance Control Panel
activationclient.dll	10.0.19041.1	Activation Client
activationmanager.dll	10.0.19041.488	Activation Manager
activeds.dll	10.0.19041.1	ADs Router Layer DLL
activesyncprovider.dll	10.0.19041.423	The engine that syncs ActiveSync accounts
actxprxy.dll	10.0.19041.488	ActiveX Interface Marshaling Library
acwinrt.dll	10.0.19041.1	Windows Compatibility DLL
acwow64.dll	10.0.19041.423	Windows Compatibility for 32bit Apps on Win64
acxtrnal.dll	10.0.19041.1	Windows Compatibility DLL
adaptivecards.dll	10.0.19041.1	Windows Adaptive Cards API Server
addressparser.dll	10.0.19041.1	ADDRESSPARSER
admtmpl.dll	10.0.19041.1	Administrative Templates Extension
adprovider.dll	10.0.19041.1	adprovider DLL
adrclient.dll	10.0.19041.1	Microsoft® Access Denied Remediation Client
adsldp.dll	10.0.19041.1	ADs LDAP Provider DLL

Navigation

adsldpc.dll	10.0.19041.1	ADs LDAP Provider C DLL
adsmsext.dll	10.0.19041.1	ADs LDAP Provider DLL
adsnt.dll	10.0.19041.1	ADs Windows NT Provider DLL
adtschema.dll	10.0.19041.1	Security Audit Schema DLL
advapi32.dll	10.0.19041.1	Advanced Windows 32 Base API
advapi32res.dll	10.0.19041.1	Advanced Windows 32 Base API
advpack.dll	11.0.19041.1	ADVPACK
aeevts.dll	10.0.19041.1	Application Experience Event Resources
aepic.dll	10.0.19041.388	Application Experience Program Cache
agentactivationruntime.dll	10.0.19041.423	Agent Activation Runtime Common DLL
agentactivationruntimewindows.dll	10.0.19041.423	Agent Activation Runtime Windows DLL
altspace.dll	10.0.19041.1	
amsi.dll	10.0.19041.1	Anti-Malware Scan Interface
amstream.dll	10.0.19041.1	DirectShow Runtime.
analogcommonproxystub.dll	10.0.19041.1	Analog Common Proxy Stub
apds.dll	10.0.19041.1	Microsoft® Help Data Services Module
aphostclient.dll	10.0.19041.1	Accounts Host Service RPC Client
apisethost.appexecutionalias.dll	10.0.19041.264	ApiSetHost.AppExecutionAlias
appcontracts.dll	10.0.19041.488	Windows AppContracts API Server
appextension.dll	10.0.19041.388	AppExtension API
apphelp.dll	10.0.19041.1	Application Compatibility Client Library
apphlpdm.dll	10.0.19041.1	Application Compatibility Help Module
appidapi.dll	10.0.19041.1	Application Identity APIs Dll
appidpolicyengineapi.dll	10.0.19041.1	AppId Policy Engine API Module
appinstallerprompt.desktop.dll	10.0.19041.1	AppInstaller Prompt Desktop
applockercsp.dll	10.0.19041.488	AppLockerCSP
appmanagementconfiguration.dll	10.0.19041.1	Application Management Configuration
appmgmts.dll	10.0.19041.1	Software installation Service
appmgr.dll	10.0.19041.1	Software Installation Snapin Extenstion
appointmentactivation.dll	10.0.19041.388	DLL for AppointmentActivation
appointmentapis.dll	10.0.19041.264	DLL for CalendarRT
apprepapi.dll	10.0.19041.1	Application Reputation APIs Dll
appresolver.dll	10.0.19041.264	App Resolver
appvclientps.dll	10.0.19041.1	Microsoft Application Virtualization Client API Proxy Stub
appventsubsystems32.dll	10.0.19041.488	Client Virtualization Subsystems
appvsentinel.dll	10.0.19041.1	Microsoft Application Virtualization Client Sentinel DLL
appvterminator.dll	10.0.19041.1	Microsoft Application Virtualization Terminator
appxalluserstore.dll	10.0.19041.488	AppX All User Store DLL
appxapplicabilityengine.dll	10.0.19041.508	AppX Applicability Engine
appxdeploymentclient.dll	10.0.19041.488	AppX Deployment Client DLL
appxpackaging.dll	10.0.19041.1	Native Code Appx Packaging Library
appxsip.dll	10.0.19041.1	Appx Subject Interface Package
archiveint.dll	3.3.2.0	Windows-internal libarchive library
asferror.dll	12.0.19041.1	ASF Error Definitions
aspnet_counters.dll	4.8.4084.0	Microsoft ASP.NET Performance Counter Shim DLL
assignedaccessruntime.dll	10.0.19041.488	AssignedAccessRuntime
asycfilt.dll	10.0.19041.1	ASYCFILT.DLL
atl.dll	3.5.2284.0	ATL Module for Windows XP (Unicode)
atl100.dll	10.0.40219.325	ATL Module for Windows
atl110.dll	11.0.60610.1	ATL Module for Windows
atlthunk.dll	10.0.19041.329	atlthunk.dll
atmlib.dll	5.1.2.254	Windows NT OpenType/Type 1 API Library.
audiodev.dll	10.0.19041.1	Portable Media Devices Shell Extension
audioeng.dll	10.0.19041.1	Audio Engine
audiokse.dll	10.0.19041.1	Audio Ks Endpoint

Navigation

audioses.dll	10.0.19041.264	Audio Session
auditnativesnapin.dll	10.0.19041.1	Audit Policy Group Policy Editor Extension
auditpolcore.dll	10.0.19041.1	Audit Policy Program
auditpolicygpinterop.dll	10.0.19041.1	Audit Policy GP Module
auditpolmsg.dll	10.0.19041.1	Audit Policy MMC SnapIn Messages
authbroker.dll	10.0.19041.264	Web Authentication WinRT API
authbrokerui.dll	10.0.19041.1	AuthBroker UI
authext.dll	10.0.19041.1	Authentication Extensions
authfwcfg.dll	10.0.19041.1	Windows Defender Firewall with Advanced Security Configuration Helper
authfwgp.dll	10.0.19041.1	Windows Defender Firewall with Advanced Security Group Policy Editor Extension
authfwsnapin.dll	10.0.19041.1	Microsoft.WindowsFirewall.SnapIn
authfwwizfwk.dll	10.0.19041.1	Wizard Framework
authui.dll	10.0.19041.388	Windows Authentication UI
authz.dll	10.0.19041.1	Authorization Framework
autoplay.dll	10.0.19041.423	AutoPlay Control Panel
avicap32.dll	10.0.19041.1	AVI Capture window class
avifil32.dll	10.0.19041.1	Microsoft AVI File support library
avrt.dll	10.0.19041.1	Multimedia Realtime Runtime
azroles.dll	10.0.19041.329	azroles Module
azroleui.dll	10.0.19041.1	Authorization Manager
azsqlext.dll	10.0.19041.1	AzMan Sql Audit Extended Stored Procedures Dll
azuresettingsyncprovider.dll	10.0.19041.1	Azure Setting Sync Provider
backgroundmediapolicy.dll	10.0.19041.1	<d> Background Media Policy DLL
bamsettingsclient.dll	10.0.19041.1	Background Activity Moderator Settings Client
basecsp.dll	10.0.19041.1	Microsoft Base Smart Card Crypto Provider
batmeter.dll	10.0.19041.1	Battery Meter Helper DLL
bcastdvr.proxy.dll	10.0.19041.1	Broadcast DVR Proxy
bcastdvrbroker.dll	10.0.19041.264	Windows Runtime BcastDVRBroker DLL
bcastdvrclient.dll	10.0.19041.264	Windows Runtime BcastDVRClient DLL
bcastdvrcommon.dll	10.0.19041.1	Windows Runtime BcastDVRCommon DLL
bcd.dll	10.0.19041.1	BCD DLL
bcp47langs.dll	10.0.19041.1	BCP47 Language Classes
bcp47mrm.dll	10.0.19041.1	BCP47 Language Classes for Resource Management
bcrypt.dll	10.0.19041.1	Windows Cryptographic Primitives Library
bcryptprimitives.dll	10.0.19041.264	Windows Cryptographic Primitives Library
bidispl.dll	10.0.19041.1	Bidispl DLL
bingmaps.dll	10.0.19041.388	Bing Map Control
bingonlineservices.dll	10.0.19041.1	Bing online services
biocredprov.dll	10.0.19041.423	WinBio Credential Provider
bitlockercsp.dll	10.0.19041.488	BitLockerCSP
bitsperf.dll	7.8.19041.1	Perfmon Counter Access
bitsproxy.dll	7.8.19041.1	Background Intelligent Transfer Service Proxy
biwinrt.dll	10.0.19041.1	Windows Background Broker Infrastructure
bluetoothapis.dll	10.0.19041.1	Bluetooth Usermode Api host
bootvid.dll	10.0.19041.1	VGA Boot Driver
browcli.dll	10.0.19041.1	Browser Service Client DLL
browsersettingsync.dll	10.0.19041.1	Browser Setting Synchronization
browseui.dll	10.0.19041.1	Shell Browser UI Library
btagservice.dll	10.0.19041.488	Bluetooth Audio Gateway Service
bthtelemetry.dll	10.0.19041.1	Bluetooth Telemetry Agent
btpanui.dll	10.0.19041.1	Bluetooth PAN User Interface
bwcontexthandler.dll	1.0.0.1	ContextH Application
c_g18030.dll	10.0.19041.1	GB18030 DBCS-Unicode Conversion DLL
c_gsm7.dll	10.0.19041.1	GSM 7bit Code Page Translation DLL for SMS
c_is2022.dll	10.0.19041.1	ISO-2022 Code Page Translation DLL

Navigation

c_iscii.dll	10.0.19041.1	ISCII Code Page Translation DLL
cabapi.dll	10.0.19041.1	Mobile Cabinet Library
cabinet.dll	5.0.1.1	Microsoft® Cabinet File API
cabview.dll	10.0.19041.1	Cabinet File Viewer Shell Extension
callbuttons.dll	10.0.19041.1	Windows Runtime CallButtonsServer DLL
callbuttons.proxystub.dll	10.0.19041.1	Windows Runtime CallButtonsServer ProxyStub DLL
callhistoryclient.dll	10.0.19041.1	Client DLL for accessing CallHistory information
cameracaptureui.dll	10.0.19041.388	Microsoft® Windows® Operating System
capabilityaccessmanagerclient.dll	10.0.19041.388	Capability Access Manager Client
capauthz.dll	10.0.19041.1	Capability Authorization APIs
capiprovider.dll	10.0.19041.1	capiprovider DLL
capisp.dll	10.0.19041.1	Sysprep cleanup dll for CAPI
castingshellext.dll	10.0.19041.1	Casting Shell Extensions
catsrv.dll	2001.12.10941.16384	COM+ Configuration Catalog Server
catsrvps.dll	2001.12.10941.16384	COM+ Configuration Catalog Server Proxy/Stub
catsrvut.dll	2001.12.10941.16384	COM+ Configuration Catalog Server Utilities
cca.dll	10.0.19041.1	CCA DirectShow Filter.
cdosys.dll	6.6.19041.329	Microsoft CDO for Windows Library
cdp.dll	10.0.19041.488	Microsoft (R) CDP Client API
cdprt.dll	10.0.19041.488	Microsoft (R) CDP Client WinRT API
cemapi.dll	10.0.19041.1	CEMAPI
certca.dll	10.0.19041.1	Microsoft® Active Directory Certificate Services CA
certcli.dll	10.0.19041.1	Microsoft® Active Directory Certificate Services Client
certcredprovider.dll	10.0.19041.1	Cert Credential Provider
certenc.dll	10.0.19041.1	Active Directory Certificate Services Encoding
certenroll.dll	10.0.19041.329	Microsoft® Active Directory Certificate Services Enrollment Client
certenrollui.dll	10.0.19041.1	X509 Certificate Enrollment UI
certmgr.dll	10.0.19041.1	Certificates snap-in
certpkicmdlet.dll	10.0.19041.1	Microsoft® PKI Client Cmdlets
certpoleng.dll	10.0.19041.1	Certificate Policy Engine
cewmdm.dll	12.0.19041.1	Windows CE WMDM Service Provider
cfgbkend.dll	10.0.19041.1	Configuration Backend Interface
cfgmgr32.dll	10.0.19041.1	Configuration Manager DLL
cfmifs.dll	10.0.19041.1	FmIfs Engine
cfmifsproxy.dll	10.0.19041.1	Microsoft® FmIfs Proxy Library
chakra.dll	11.0.19041.508	Microsoft ® Chakra (Private)
chakradiag.dll	11.0.19041.508	Microsoft ® Chakra Diagnostics (Private)
chakrathunk.dll	10.0.19041.508	chakrathunk.dll
chartv.dll	10.0.19041.1	Chart View
chatapis.dll	10.0.19041.264	DLL for ChatRT
chxreadingstringime.dll	10.0.19041.1	CHxReadingStringIME
cic.dll	10.0.19041.329	CIC - MMC controls for Taskpad
ciwmi.dll	10.0.19041.1	WMIv2 Provider for CI Policy Management
clb.dll	10.0.19041.1	Column List Box
clbcatq.dll	2001.12.10941.16384	COM+ Configuration Catalog
cldapi.dll	10.0.19041.1	Cloud API user mode API
clfsw32.dll	10.0.19041.21	Common Log Marshalling Win32 DLL
cliconfg.dll	10.0.19041.1	SQL Client Configuration Utility DLL
clipboardserver.dll	10.0.19041.1	Modern Clipboard API Server
clipc.dll	10.0.19041.508	Client Licensing Platform Client
cloudexperiencehostcommon.dll	10.0.19041.508	CloudExperienceHostCommon
cloudexperiencehostuser.dll	10.0.19041.423	CloudExperienceHost User Operations
clrhost.dll	10.0.19041.1	In Proc server for managed servers in the Windows Runtime
clusapi.dll	10.0.19041.488	Cluster API Library
cmcfg32.dll	7.2.19041.1	Microsoft Connection Manager Configuration Dll

Navigation

cmdext.dll	10.0.19041.1	cmd.exe Extension DLL
cmdial32.dll	7.2.19041.1	Microsoft Connection Manager
cmgrcspps.dll	10.0.19041.1	cmgrcspps
cmifw.dll	10.0.19041.1	Windows Defender Firewall rule configuration plug-in
cmintegrator.dll	10.0.19041.488	cmintegrator.dll
cmlua.dll	7.2.19041.1	Connection Manager Admin API Helper
cmpbk32.dll	7.2.19041.1	Microsoft Connection Manager Phonebook
cmstplua.dll	7.2.19041.1	Connection Manager Admin API Helper for Setup
cmutil.dll	7.2.19041.1	Microsoft Connection Manager Utility Lib
cngcredui.dll	10.0.19041.1	Microsoft CNG CredUI Provider
cngprovider.dll	10.0.19041.1	cngprovider DLL
cnvfat.dll	10.0.19041.1	FAT File System Conversion Utility DLL
colbact.dll	2001.12.10941.16384	COM+
coloradapterclient.dll	10.0.19041.264	Microsoft Color Adapter Client
colorcnv.dll	10.0.19041.1	Windows Media Color Conversion
colorui.dll	10.0.19041.1	Microsoft Color Control Panel
combase.dll	10.0.19041.508	Microsoft COM for Windows
comcat.dll	10.0.19041.1	Microsoft Component Category Manager Library
comctl32.dll	5.82.19041.488	User Experience Controls Library
comdlg32.dll	10.0.19041.488	Common Dialogs DLL
coml2.dll	10.0.19041.1	Microsoft COM for Windows
compobj.dll	3.10.0.103	Windows Win16 Application Launcher
composableshellproxystub.dll	10.0.19041.1	Composable Shell Shared Proxy Stub
comppkgsup.dll	10.0.19041.1	Component Package Support DLL
compstui.dll	10.0.19041.423	Common Property Sheet User Interface DLL
comrepl.dll	2001.12.10941.16384	COM+
comres.dll	2001.12.10941.16384	COM+ Resources
comsnap.dll	2001.12.10941.16384	COM+ Explorer MMC Snapin
comsvcs.dll	2001.12.10941.16384	COM+ Services
comuid.dll	2001.12.10941.16384	COM+ Explorer UI
concrt140.dll	14.24.28127.4	Microsoft® Concurrency Runtime Library
configureexpandedstorage.dll	10.0.19041.264	ConfigureExpandedStorage
connect.dll	10.0.19041.1	Get Connected Wizards
connectedaccountstate.dll	10.0.19041.1	ConnectedAccountState.dll
console.dll	10.0.19041.1	Control Panel Console Applet
consolelogon.dll	10.0.19041.388	Console Logon User Experience
contactactivation.dll	10.0.19041.1	DLL for ContactActivation
contactapis.dll	10.0.19041.264	DLL for ContactsRT
container.dll	10.0.19041.292	Windows Containers
contentdeliverymanager.utilities.dll	10.0.19041.423	ContentDeliveryManager.Utilities
coreglobconfig.dll	10.0.19041.388	Core Globalization Configuration
coremas.dll		
coremessaging.dll	10.0.19041.423	Microsoft CoreMessaging Dll
coremmres.dll	10.0.19041.1	General Core Multimedia Resources
coreshellapi.dll	10.0.19041.388	CoreShellAPI
coreuicomponents.dll	10.0.19041.1	Microsoft Core UI Components Dll
cpfilters.dll	10.0.19041.508	PTFilter & Encypter/Decrypter Tagger Filters.
credprov2fahelper.dll	10.0.19041.1	Credential Provider 2FA Helper
credprovdatamodel.dll	10.0.19041.388	Cred Prov Data Model
credprovhelper.dll	10.0.19041.1	Credential Provider Helper
credprovhost.dll	10.0.19041.1	Credential Provider Framework Host
credprovs.dll	10.0.19041.488	Credential Providers
credprovslegacy.dll	10.0.19041.1	Credential Providers Legacy
credssp.dll	10.0.19041.264	Credential Delegation Security Package
credui.dll	10.0.19041.1	Credential Manager User Interface

Navigation

crtdll.dll	4.0.1183.1	Microsoft C Runtime Library
crypt32.dll	10.0.19041.21	Crypto API32
cryptbase.dll	10.0.19041.1	Base cryptographic API DLL
cryptdlg.dll	10.0.19041.1	Microsoft Common Certificate Dialogs
cryptdll.dll	10.0.19041.1	Cryptography Manager
cryptext.dll	10.0.19041.1	Crypto Shell Extensions
cryptnet.dll	10.0.19041.1	Crypto Network Related API
cryptngc.dll	10.0.19041.423	Microsoft Passport API
cryptowinrt.dll	10.0.19041.1	Crypto WinRT Library
cryptsp.dll	10.0.19041.1	Cryptographic Service Provider API
crypttpmeksvc.dll	10.0.19041.1	Cryptographic TPM Endorsement Key Services
cryptui.dll	10.0.19041.264	Microsoft Trust UI Provider
cryptuiwizard.dll	10.0.19041.1	Microsoft Trust UI Provider
cryptxml.dll	10.0.19041.1	XML DigSig API
cscapi.dll	10.0.19041.1	Offline Files Win32 API
cscdll.dll	10.0.19041.1	Offline Files Temporary Shim
cscobj.dll	10.0.19041.1	In-proc COM object used by clients of CSC API
ctl3d32.dll	2.31.0.0	Ctl3D 3D Windows Controls
d2d1.dll	10.0.19041.329	Microsoft D2D Library
d3d10.dll	10.0.19041.1	Direct3D 10 Runtime
d3d10_1.dll	10.0.19041.1	Direct3D 10.1 Runtime
d3d10_1core.dll	10.0.19041.1	Direct3D 10.1 Runtime
d3d10core.dll	10.0.19041.1	Direct3D 10 Runtime
d3d10level9.dll	10.0.19041.1	Direct3D 10 to Direct3D9 Translation Runtime
d3d10warp.dll	10.0.19041.1	Direct3D Rasterizer
d3d11.dll	10.0.19041.1	Direct3D 11 Runtime
d3d11on12.dll	10.0.19041.1	Direct3D 11On12 Runtime
d3d12.dll	10.0.19041.423	Direct3D 12 Runtime
d3d8.dll	10.0.19041.1	Microsoft Direct3D
d3d8thk.dll	10.0.19041.488	Microsoft Direct3D OS Thunk Layer
d3d9.dll	10.0.19041.488	Direct3D 9 Runtime
d3d9on12.dll	10.0.19041.1	Direct3D9 DDI to Direct3D12 API Mapping Layer
d3dcompiler_43.dll	9.29.952.3111	Direct3D HLSL Compiler
d3dcompiler_47.dll	10.0.19041.1	Direct3D HLSL Compiler
d3dcsx_43.dll	9.29.952.3111	Direct3D 10.1 Extensions
d3dim.dll	10.0.19041.1	Microsoft Direct3D
d3dim700.dll	10.0.19041.1	Microsoft Direct3D
d3dramp.dll	10.0.19041.1	Microsoft Direct3D
d3dscache.dll	10.0.19041.1	Microsoft (R) D3D Shader Caching Library
d3dx10_43.dll	9.29.952.3111	Direct3D 10.1 Extensions
d3dx11_43.dll	9.29.952.3111	Direct3D 10.1 Extensions
d3dx9_30.dll	9.12.589.0	Microsoft® DirectX for Windows®
d3dx9_43.dll	9.29.952.3111	Direct3D 9 Extensions
d3dxof.dll	10.0.19041.1	DirectX Files DLL
dabapi.dll	10.0.19041.1	Desktop Activity Broker API
dafprintprovider.dll	10.0.19041.423	DAF Print Provider DLL
daotpcredentialprovider.dll	10.0.19041.1	DirectAccess One-Time Password Credential Provider
dataclen.dll	10.0.19041.1	Disk Space Cleaner for Windows
dataexchange.dll	10.0.19041.264	Data exchange
davclnt.dll	10.0.19041.1	Web DAV Client DLL
davhlpr.dll	10.0.19041.1	DAV Helper DLL
davsyncprovider.dll	10.0.19041.1	DAV sync engine for contacts, calendar
daxexec.dll	10.0.19041.488	daxexec
dbgcore.dll	10.0.19041.1	Windows Core Debugging Helpers
dbgeng.dll	10.0.19041.1	Windows Symbolic Debugger Engine

Navigation

dbghelp.dll	10.0.19041.488	Windows Image Helper
dbgmodel.dll	10.0.19041.1	Windows Debugger Data Model
dbnetlib.dll	10.0.19041.1	Winsock Oriented Net DLL for SQL Clients
dbnmpntw.dll	10.0.19041.1	Named Pipes Net DLL for SQL Clients
dciman32.dll	10.0.19041.508	DCI Manager
dcomp.dll	10.0.19041.488	Microsoft DirectComposition Library
ddaclsys.dll	10.0.19041.1	SysPrep module for Resetting Data Drive ACL
ddisplay.dll	10.0.19041.1	DirectDisplay
ddoiproxy.dll	10.0.19041.1	DDOI Interface Proxy
ddores.dll	10.0.19041.1	Device Category information and resources
ddraw.dll	10.0.19041.1	Microsoft DirectDraw
ddrawex.dll	10.0.19041.1	Direct Draw Ex
defaultdevicemanager.dll	10.0.19041.1	Default Device Manager
defaultprinterprovider.dll	10.0.19041.1	Microsoft Windows Default Printer Provider
delegatorprovider.dll	10.0.19041.1	WMI PassThru Provider for Storage Management
desktopshellappstatecontract.dll	10.0.19041.1	Desktop Switcher Data Model
devdispitemprovider.dll	10.0.19041.1	DeviceItem inproc devquery subsystem
devenum.dll	10.0.19041.329	Device enumeration.
deviceaccess.dll	10.0.19041.264	Device Broker And Policy COM Server
deviceassociation.dll	10.0.19041.1	Device Association Client DLL
devicecenter.dll	10.0.19041.1	Device Center
devicecredential.dll	10.0.19041.1	Microsoft Companion Authenticator Client
devicedisplaystatusmanager.dll	10.0.19041.1	Device Display Status Manager
deviceflows.datamodel.dll	10.0.19041.1	DeviceFlows DataModel
devicengccredprov.dll	10.0.19041.1	Microsoft Companion Authenticator Credential Provider
devicepairing.dll	10.0.19041.1	Shell extensions for Device Pairing
devicepairingfolder.dll	10.0.19041.1	Device Pairing Folder
devicepairingproxy.dll	10.0.19041.1	Device Pairing Proxy Dll
devicereactivation.dll	10.0.19041.488	DeviceReactivation
devicesetupstatusprovider.dll	10.0.19041.1	Device Setup Status Provider Dll
deviceuxres.dll	10.0.19041.1	Windows Device User Experience Resource File
devmgr.dll	10.0.19041.1	Device Manager MMC Snapin
devobj.dll	10.0.19041.1	Device Information Set DLL
devrtl.dll	10.0.19041.1	Device Management Run Time Library
dfscli.dll	10.0.19041.1	Windows NT Distributed File System Client DLL
dfshim.dll	10.0.19041.1	ClickOnce Application Deployment Support Library
dfsshlex.dll	10.0.19041.1	Distributed File System shell extension
dhcpcmonitor.dll	10.0.19041.1	DHCP Client Monitor Dll
dhcpcore.dll	10.0.19041.508	DHCP Client Service
dhcpcore6.dll	10.0.19041.508	DHCPv6 Client
dhcpcsvc.dll	10.0.19041.508	DHCP Client Service
dhcpcsvc6.dll	10.0.19041.508	DHCPv6 Client
dhcpsapi.dll	10.0.19041.1	DHCP Server API Stub DLL
diagnosticdataquery.dll	10.0.19041.1	Microsoft Windows Diagnostic data Helper API
diagnosticinvoker.dll	10.0.19041.388	Microsoft Windows operating system.
dialclient.dll	10.0.19041.488	DIAL DLL
dictationmanager.dll	10.0.0.1	Dictation Manager
difxapi.dll	2.1.0.0	Driver Install Frameworks for API library module
dimsjob.dll	10.0.19041.1	DIMS Job DLL
dimsroam.dll	10.0.19041.1	Key Roaming DIMS Provider DLL
dinput.dll	10.0.19041.1	Microsoft DirectInput
dinput8.dll	10.0.19041.1	Microsoft DirectInput
direct2ddesktop.dll	10.0.19041.1	Microsoft Direct2D Desktop Components
directmanipulation.dll	10.0.19041.1	Microsoft Direct Manipulation Component
directml.dll	1.0.2007.1310	DirectML Library

Navigation

dismapi.dll	10.0.19041.329	DISM API Framework
dispbroker.dll	10.0.19041.1	Display Broker API
dispex.dll	5.812.10240.16384	Microsoft ® DispEx
display.dll	10.0.19041.1	Display Control Panel
displaymanager.dll	10.0.19041.1	DisplayManager
dlnashext.dll	10.0.19041.1	DLNA Namespace DLL
dmalertlistener.proxystub.dll	10.0.19041.488	ProxyStub for DeviceManagment Alert
dmappsres.dll	10.0.19041.1	DMAppsRes
dmband.dll	10.0.19041.1	Microsoft DirectMusic Band
dmcfgutils.dll	10.0.19041.423	dmcfgutils
dmcmnutils.dll	10.0.19041.423	dmcmnutils
dmcommandlineutils.dll	10.0.19041.1	dmcommandlineutils
dmcompos.dll	10.0.19041.1	Microsoft DirectMusic Composer
dmdlgs.dll	10.0.19041.1	Disk Management Snap-in Dialogs
dmdskmgr.dll	10.0.19041.1	Disk Management Snap-in Support Library
dmdskres.dll	10.0.19041.1	Disk Management Snap-in Resources
dmdskres2.dll	10.0.19041.1	Disk Management Snap-in Resources
dmenrollengine.dll	10.0.19041.488	Enroll Engine DLL
dmime.dll	10.0.19041.1	Microsoft DirectMusic Interactive Engine
dmintf.dll	10.0.19041.1	Disk Management DCOM Interface Stub
dmiso8601utils.dll	10.0.19041.1	dmiso8601utils
dmloader.dll	10.0.19041.1	Microsoft DirectMusic Loader
dmocx.dll	10.0.19041.1	TreeView OCX
dmoleaututils.dll	10.0.19041.1	dmoleaututils
dmprocessxmlfiltered.dll	10.0.19041.1	dmprocessxmlfiltered
dmpushproxy.dll	10.0.19041.1	dmpushproxy
dmrcdecoder.dll	1.0.0.30	Digimarc Decoder 11/8/2017 6:30 AM [TGNP4W2UT0BB8JC]
dmscript.dll	10.0.19041.1	Microsoft DirectMusic Scripting
dmstyle.dll	10.0.19041.1	Microsoft DirectMusic Style Engline
dmsynth.dll	10.0.19041.1	Microsoft DirectMusic Software Synthesizer
dmusic.dll	10.0.19041.1	Microsoft DirectMusic Core Services
dmutil.dll	10.0.19041.1	Logical Disk Manager Utility Library
dmvdsitf.dll	10.0.19041.1	Disk Management Snap-in Support Library
dmxmlhelputils.dll	10.0.19041.1	dmxmlhelputils
dnsapi.dll	10.0.19041.508	DNS Client API DLL
dnscmmc.dll	10.0.19041.1	DNS Client MMC Snap-in DLL
docprop.dll	10.0.19041.1	OLE DocFile Property Page
dolbydecmft.dll	10.0.19041.488	Media Foundation Dolby Digital Atmos Decoders
dot3api.dll	10.0.19041.488	802.3 Autoconfiguration API
dot3cfg.dll	10.0.19041.1	802.3 Netsh Helper
dot3dlg.dll	10.0.19041.1	802.3 UI Helper
dot3gpclnt.dll	10.0.19041.1	802.3 Group Policy Client
dot3gpui.dll	10.0.19041.1	802.3 Network Policy Management Snap-in
dot3hc.dll	10.0.19041.1	Dot3 Helper Class
dot3msm.dll	10.0.19041.488	802.3 Media Specific Module
dot3ui.dll	10.0.19041.1	802.3 Advanced UI
dpapi.dll	10.0.19041.1	Data Protection API
dpapiprovider.dll	10.0.19041.1	dpapiprovider DLL
dplayx.dll	10.0.19041.1	DirectPlay Stub
dpmodemx.dll	10.0.19041.1	DirectPlay Stub
dpnaddr.dll	10.0.19041.1	DirectPlay Stub
dpnathlp.dll	10.0.19041.1	DirectPlay Stub
dpnet.dll	10.0.19041.1	DirectPlay Stub
dpnhpast.dll	10.0.19041.1	DirectPlay Stub
dpnhupnp.dll	10.0.19041.1	DirectPlay Stub

dpnlobby.dll	10.0.19041.1	DirectPlay Stub
dpwsockx.dll	10.0.19041.1	DirectPlay Stub
dpx.dll	10.0.19041.1	Microsoft(R) Delta Package Expander
dragdropexperiencecommon.dll	10.0.19041.1	In-Proc WinRT server for Windows.Internal.PlatformExtensions.DragDropExperienceCommon
dragdropexperiencedataexchangedelegated.dll	10.0.19041.1	In-Proc WinRT server for Windows.Internal.PlatformExtensions.DragDropExperienceDataExchangeDelegated
drprov.dll	10.0.19041.1	Microsoft Remote Desktop Session Host Server Network Provider
drt.dll	10.0.19041.1	Distributed Routing Table
drtprov.dll	10.0.19041.1	Distributed Routing Table Providers
drttransport.dll	10.0.19041.1	Distributed Routing Table Transport Provider
drvsetup.dll	10.0.19041.423	Microsoft (R) Driver Setup
drvstore.dll	10.0.19041.488	Driver Store API
dsauth.dll	10.0.19041.1	DS Authorization for Services
dsccoreconfprov.dll	6.2.9200.16384	DSC
dsclient.dll	10.0.19041.1	Data Sharing Service Client DLL
dsdmo.dll	10.0.19041.1	DirectSound Effects
dskquota.dll	10.0.19041.1	Windows Shell Disk Quota Support DLL
dskquoui.dll	10.0.19041.1	Windows Shell Disk Quota UI DLL
dsound.dll	10.0.19041.1	DirectSound
dsparse.dll	10.0.19041.1	Active Directory Domain Services API
dsprop.dll	10.0.19041.1	Windows Active Directory Property Pages
dsquery.dll	10.0.19041.1	Directory Service Find
dsreg.dll	10.0.19041.1	AD/AAD User Device Registration
dsregtask.dll	10.0.19041.1	DSREG task handler
dsrole.dll	10.0.19041.1	DS Setup Client DLL
dssec.dll	10.0.19041.1	Directory Service Security UI
dssenh.dll	10.0.19041.1	Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
dsui.dll	10.0.19041.423	Device Setup UI Pages
dsuiext.dll	10.0.19041.1	Directory Service Common UI
dswave.dll	10.0.19041.1	Microsoft DirectMusic Wave
dtsh.dll	10.0.19041.1	Detection and Sharing Status API
dui70.dll	10.0.19041.1	Windows DirectUI Engine
duser.dll	10.0.19041.1	Windows DirectUser Engine
dusmapi.dll	10.0.19041.1	Data Usage API
dwmapi.dll	10.0.19041.488	Microsoft Desktop Window Manager API
dwrite.dll	10.0.19041.388	Microsoft DirectX Typography Services
dxcore.dll	10.0.19041.1	DXCore
dxdiagn.dll	10.0.19041.488	Microsoft DirectX Diagnostic Tool
dxgi.dll	10.0.19041.488	DirectX Graphics Infrastructure
dxilconv.dll	10.0.19041.1	DirectX IL Converter DLL
dxptasksync.dll	10.0.19041.423	Microsoft Windows DXP Sync.
dxtmsft.dll	11.0.19041.1	DirectX Media -- Image DirectX Transforms
dxtrans.dll	11.0.19041.329	DirectX Media -- DirectX Transform Core
dxva2.dll	10.0.19041.1	DirectX Video Acceleration 2.0 DLL
eapp3hst.dll	10.0.19041.1	Microsoft ThirdPartyEapDispatcher
eappcfg.dll	10.0.19041.1	Eap Peer Config
eappgnui.dll	10.0.19041.1	EAP Generic UI
eapphost.dll	10.0.19041.1	Microsoft EAPHost Peer service
eappprxy.dll	10.0.19041.1	Microsoft EAPHost Peer Client DLL
eapprovp.dll	10.0.19041.1	EAP extension DLL
eapputil.dll	10.0.19041.1	EAP Private Utility DLL
eapsimextdesktop.dll	10.0.19041.1	EAP SIM EXT config dll
eapteapconfig.dll	10.0.19041.1	EAP Teap Config DLL
eapteapext.dll	10.0.19041.1	EAP Teap Desktop Extension DLL
easwrt.dll	10.0.19041.388	Exchange ActiveSync Windows Runtime DLL
edgehtml.dll	11.0.19041.508	Microsoft Edge Web Platform

Navigation

Navigation

edgeiso.dll	11.0.19041.488	Isolation Library for edgehtml hosts
edgemanager.dll	11.0.19041.423	Microsoft Edge Manager
editbuffertesthook.dll	10.0.19041.508	"EditBufferTestHook.DYNLINK"
editionupgradehelper.dll	10.0.19041.488	EDITIONUPGRADEHELPER.DLL
editionupgrademanagerobj.dll	10.0.19041.488	Get your Windows license
edpauditapi.dll	10.0.19041.1	EDP Audit API
edputil.dll	10.0.19041.1	EDP util
efsadu.dll	10.0.19041.1	File Encryption Utility
efsext.dll	10.0.19041.1	EFSEXT.DLL
efsutil.dll	10.0.19041.1	EFS Utility Library
efswrt.dll	10.0.19041.488	Storage Protection Windows Runtime DLL
ehstorapi.dll	10.0.19041.1	Windows Enhanced Storage API
ehstorpwdmgr.dll	10.0.19041.1	Microsoft Enhanced Storage Password Manager
els.dll	10.0.19041.1	Event Viewer Snapin
elscore.dll	10.0.19041.1	Els Core Platform DLL
elshyph.dll	10.0.19041.1	ELS Hyphenation Service
elslad.dll	10.0.19041.1	ELS Language Detection
elstrans.dll	10.0.19041.1	ELS Transliteration Service
emailapis.dll	10.0.19041.264	DLL for EmailRT
embeddedmodesvcapi.dll	10.0.19041.1	Embedded Mode Service Client DLL
encapi.dll	10.0.19041.1	Encoder API
enrollmentapi.dll	10.0.19041.488	Legacy Phone Enrollment API BackCompat Shim
enterpriseappmgmtclient.dll	10.0.19041.1	EnterpriseAppMgmtClient.dll
enterpriseresourcemanager.dll	10.0.19041.423	enterpriseresourcemanager DLL
eqossnap.dll	10.0.19041.1	EQoS Snapin extension
errordetails.dll	10.0.19041.388	Microsoft Windows operating system.
errordetailscore.dll	10.0.19041.1	Microsoft Windows operating system.
es.dll	2001.12.10941.16384	COM+
esdsip.dll	10.0.19041.1	Crypto SIP provider for signing and verifying .esd Electronic Software Distribution files
esent.dll	10.0.19041.1	Extensible Storage Engine for Microsoft(R) Windows(R)
esentprf.dll	10.0.19041.1	Extensible Storage Engine Performance Monitoring Library for Microsoft(R) Windows(R)
esevss.dll	10.0.19041.1	Microsoft(R) ESENT shadow utilities
etwcoreuicomponentsresources.dll	10.0.19041.1	Microsoft CoreComponents UI ETW manifest Dll
etweseproviderresources.dll	10.0.19041.1	Microsoft ESE ETW
etwrundown.dll	10.0.19041.1	Etw Rundown Helper Library
eventcls.dll	10.0.19041.1	Microsoft® Volume Shadow Copy Service event class
evr.dll	10.0.19041.1	Enhanced Video Renderer DLL
execmodelclient.dll	10.0.19041.264	ExecModelClient
execmodelproxy.dll	10.0.19041.1	ExecModelProxy
explorerframe.dll	10.0.19041.488	ExplorerFrame
expsrv.dll	6.0.72.9589	Visual Basic for Applications Runtime - Expression Service
exsmime.dll	10.0.19041.1	LExsmime
extrasxmlparser.dll	10.0.19041.1	Extras XML parser used to extract extension information from XML
f3ahvoas.dll	10.0.19041.1	JP Japanese Keyboard Layout for Fujitsu FMV oyayubi-shift keyboard
familysafetyext.dll	10.0.19041.1	FamilySafety ChildAccount Extensions
faultrep.dll	10.0.19041.388	Windows User Mode Crash Reporting DLL
fdbth.dll	10.0.19041.1	Function Discovery Bluetooth Provider Dll
fdbthproxy.dll	10.0.19041.1	Bluetooth Provider Proxy Dll
fddevquery.dll	10.0.19041.1	Microsoft Windows Device Query Helper
fde.dll	10.0.19041.1	Folder Redirection Snapin Extension
fdeploy.dll	10.0.19041.1	Folder Redirection Group Policy Extension
fdpnp.dll	10.0.19041.1	Pnp Provider Dll
fdprint.dll	10.0.19041.1	Function Discovery Print Provider Dll
fdproxy.dll	10.0.19041.1	Function Discovery Proxy Dll
fdssdp.dll	10.0.19041.508	Function Discovery SSDP Provider Dll

fdwcn.dll	10.0.19041.1	Windows Connect Now - Config Function Discover
fdwnet.dll	10.0.19041.1	Function Discovery WNet Provider Dll
fdwsd.dll	10.0.19041.508	Function Discovery WS Discovery Provider Dll
feclient.dll	10.0.19041.1	Windows NT File Encryption Client Interfaces
ffbroker.dll	10.0.19041.264	Force Feedback Broker And Policy COM Server
fidocredprov.dll	10.0.19041.1	FIDO Credential Provider
filemgmt.dll	10.0.19041.1	Services and Shared Folders
findnetprinters.dll	10.0.19041.423	Find Network Printers COM Component
fingerprintcredential.dll	10.0.19041.1	WinBio Fingerprint Credential
firewallapi.dll	10.0.19041.329	Windows Defender Firewall API
firewallcontrolpanel.dll	10.0.19041.423	Windows Defender Firewall Control Panel
flightsettings.dll	10.0.19041.488	Flight Settings
fltlib.dll	10.0.19041.1	Filter Library
fmifs.dll	10.0.19041.1	FM IFS Utility DLL
fms.dll	10.0.19041.1	Font Management Services
fontext.dll	10.0.19041.423	Windows Font Folder
fontglyphanimator.dll	10.0.19041.1	Font Glyph Animator
fontsub.dll	10.0.19041.508	Font Subsetting DLL
fphc.dll	10.0.19041.1	Filtering Platform Helper Class
framedyn.dll	10.0.19041.1	WMI SDK Provider Framework
framedynos.dll	10.0.19041.1	WMI SDK Provider Framework
frameserverclient.dll	10.0.19041.423	Frame Server Client DLL
frprov.dll	10.0.19041.1	Folder Redirection WMI Provider
fsutilext.dll	10.0.19041.1	FS Utility Extension DLL
fundisc.dll	10.0.19041.1	Function Discovery Dll
fveapi.dll	10.0.19041.488	Windows BitLocker Drive Encryption API
fveapibase.dll	10.0.19041.488	Windows BitLocker Drive Encryption Base API
fvecerts.dll	10.0.19041.1	BitLocker Certificates Library
fwbase.dll	10.0.19041.1	Firewall Base DLL
fwcfg.dll	10.0.19041.1	Windows Defender Firewall Configuration Helper
fwpolicyiomgr.dll	10.0.19041.1	FwPolicyIoMgr DLL
fwpuclnt.dll	10.0.19041.488	FWP/IPsec User-Mode API
fwremotesvr.dll	10.0.19041.1	Windows Defender Firewall Remote APIs Server
fxsapi.dll	10.0.19041.1	Microsoft Fax API Support DLL
fxscom.dll	10.0.19041.1	Microsoft Fax Server COM Client Interface
fxscomex.dll	10.0.19041.329	Microsoft Fax Server Extended COM Client Interface
fxsext32.dll	10.0.19041.1	Microsoft Fax Exchange Command Extension
fxsresm.dll	10.0.19041.1	Microsoft Fax Resource DLL
fxsxp32.dll	10.0.19041.1	Microsoft Fax Transport Provider
gamebarpresencewriter.proxy.dll	10.0.19041.1	GameBar Presence Writer Proxy
gamechatoverlayext.dll	10.0.19041.1	GameChat Overlay Extension
gamechattranscription.dll	10.0.19041.1	GameChatTranscription
gameinput.dll	0.1908.19041.508	GameInput API
gamemode.dll	10.0.19041.1	Game Mode Client
gamepanelexternalhook.dll	10.0.19041.1	GamePanelExternalHook.dll
gameux.dll	10.0.19041.1	Games Explorer
gamingtcui.dll	10.0.19041.264	Windows Gaming Internal CallableUI dll
gcdef.dll	10.0.19041.1	Game Controllers Default Sheets
gdi32.dll	10.0.19041.1	GDI Client DLL
gdi32full.dll	10.0.19041.508	GDI Client DLL
gdiplus.dll	10.0.19041.508	Microsoft GDI+
geocommon.dll	10.0.19041.1	Geocommon
geolocation.dll	10.0.19041.388	Geolocation Runtime DLL
getuname.dll	10.0.19041.1	Unicode name Dll for UCE
glmf32.dll	10.0.19041.488	OpenGL Metafiling DLL

globinputhost.dll	10.0.19041.1	Windows Globalization Extension API for Input
glu32.dll	10.0.19041.488	OpenGL Utility Library DLL
gmsaclient.dll	10.0.19041.1	"gmsaclient.DYNLINK"
gpapi.dll	10.0.19041.508	Group Policy Client API
gpedit.dll	10.0.19041.1	GPEdit
gpprefcl.dll	10.0.19041.388	Group Policy Preference Client
gpprnext.dll	10.0.19041.1	Group Policy Printer Extension
gpscript.dll	10.0.19041.1	Script Client Side Extension
gptext.dll	10.0.19041.1	GPTExt
graphicscapture.dll	10.0.19041.488	Microsoft Windows Graphics Capture Api
hbaapi.dll	10.0.19041.1	HBA API data interface dll for HBA_API_Rev_2-18_2002MAR1.doc
hcproviders.dll	10.0.19041.1	Security and Maintenance Providers
hdcphandler.dll	10.0.19041.1	Hdcp Handler DLL
heatcore.dll		
helppaneproxy.dll	10.0.19041.1	Microsoft® Help Proxy
hgcpl.dll	10.0.19041.423	HomeGroup Control Panel
hhsetup.dll	10.0.19041.1	Microsoft® HTML Help
hid.dll	10.0.19041.1	Hid User Library
hidserv.dll	10.0.19041.1	Human Interface Device Service
hlink.dll	10.0.19041.1	Microsoft Office 2000 component
hmkd.dll	10.0.19041.1	Windows HMAC Key Derivation API
hnetcfg.dll	10.0.19041.1	Home Networking Configuration Manager
hnetcfgclient.dll	10.0.19041.1	Home Networking Configuration API Client
hnetmon.dll	10.0.19041.1	Home Networking Monitor DLL
holoshellruntime.dll	10.0.19041.388	Hologram Shell Runtime
hrtfapo.dll	10.0.19041.423	HrtfApo.dll
httpapi.dll	10.0.19041.1	HTTP Protocol Stack API
htui.dll	10.0.19041.1	Common halftone Color Adjustment Dialogs
hvsimanagementapi.dll		
ia2comproxy.dll	10.0.19041.1	IAccessible2 COM Proxy Stub DLL
ias.dll	10.0.19041.1	Network Policy Server
iasacct.dll	10.0.19041.1	NPS Accounting Provider
iasads.dll	10.0.19041.329	NPS Active Directory Data Store
iasdatastore.dll	10.0.19041.1	NPS Datastore server
iashlpr.dll	10.0.19041.1	NPS Surrogate Component
iasmigplugin.dll	10.0.19041.1	NPS Migration DLL
iasnap.dll	10.0.19041.329	NPS NAP Provider
iaspolcy.dll	10.0.19041.1	NPS Pipeline
iasrad.dll	10.0.19041.1	NPS RADIUS Protocol Component
iasrecst.dll	10.0.19041.329	NPS XML Datastore Access
iassam.dll	10.0.19041.1	NPS NT SAM Provider
iassdo.dll	10.0.19041.329	NPS SDO Component
iassvcs.dll	10.0.19041.1	NPS Services Component
iccvid.dll	1.10.0.12	Cinepak® Codec
icm32.dll	10.0.19041.264	Microsoft Color Management Module (CMM)
icmp.dll	10.0.19041.1	ICMP DLL
icmui.dll	10.0.19041.1	Microsoft Color Matching System User Interface DLL
iconcodecservice.dll	10.0.19041.1	Converts a PNG part of the icon to a legacy bmp icon
icsigd.dll	10.0.19041.1	Internet Gateway Device properties
icu.dll	64.2.0.0	ICU Combined Library
icuin.dll	64.2.0.0	ICU I18N Forwarder DLL
icuuc.dll	64.2.0.0	ICU Common Forwarder DLL
idctrls.dll	10.0.19041.1	Identity Controls
idndl.dll	10.0.19041.1	Downlevel DLL
idstore.dll	10.0.19041.1	Identity Store

Navigation

Navigation

ieadvpack.dll	11.0.19041.1	ADVPACK
ieapfltr.dll	11.0.19041.329	Microsoft SmartScreen Filter
iedkcs32.dll	18.0.19041.1	IEAK branding
ieframe.dll	11.0.19041.488	Internet Browser
iemigplugin.dll	11.0.19041.488	IE Migration Plugin
iepeers.dll	11.0.19041.1	Internet Explorer Peer Objects
ieproxy.dll	11.0.19041.488	IE ActiveX Interface Marshaling Library
iernonce.dll	11.0.19041.1	Extended RunOnce processing with UI
iertutil.dll	11.0.19041.488	Run time utility for Internet Explorer
iesetup.dll	11.0.19041.1	IOD Version Map
iesysprep.dll	11.0.19041.1	IE Sysprep Provider
ieui.dll	11.0.19041.1	Internet Explorer UI Engine
ifmon.dll	10.0.19041.1	IF Monitor DLL
ifsutil.dll	10.0.19041.1	IFS Utility DLL
ifsutilx.dll	10.0.19041.1	IFS Utility Extension DLL
ig7icd32.dll	10.18.10.5129	OpenGL(R) Driver for Intel(R) Graphics Accelerator
igd10iumd32.dll	10.18.10.5129	User Mode Driver for Intel(R) Graphics Technology
igdail32.dll		
igdbcl32.dll	10.18.10.5129	OpenCL User Mode Driver for Intel(R) Graphics Technology
igdde32.dll		
igdfcl32.dll	10.18.10.5129	OpenCL User Mode Driver for Intel(R) Graphics Technology
igdmd32.dll	10.18.10.5129	Metrics Discovery API for Intel(R) Graphics Accelerator
igdrcl32.dll	10.18.10.5129	OpenCL User Mode Driver for Intel(R) Graphics Technology
igdumdim32.dll	10.18.10.5129	User Mode Driver for Intel(R) Graphics Technology
igdusc32.dll	10.18.10.5129	Unified Shader Compiler for Intel(R) Graphics Accelerator
igfx11cmrt32.dll	3.0.0.1284	MDF(CM) Runtime DX11 Dynamic Link Library
igfxcmjit32.dll	3.0.0.1284	MDF(CM) JIT Dynamic Link Library
igfxcmrt32.dll	3.0.0.1284	MDF(CM) Runtime Dynamic Link Library
igfxexps32.dll	6.15.10.5129	igfxext Module
iglhcp32.dll	9.0.20.9000	iglhcp32 Dynamic Link Library
iglhsip32.dll	9.0.20.9000	iglhsip32 Dynamic Link Library
imagehlp.dll	10.0.19041.1	Windows NT Image Helper
imageres.dll	10.0.19041.1	Windows Image Resource
imagesp1.dll	10.0.19041.1	Windows SP1 Image Resource
imapi.dll	10.0.19041.329	Image Mastering API
imapi2.dll	10.0.19041.329	Image Mastering API v2
imapi2fs.dll	10.0.19041.329	Image Mastering File System Imaging API v2
imgutil.dll	11.0.19041.1	IE plugin image decoder support DLL
imm32.dll	10.0.19041.1	Multi-User Windows IMM32 API Client DLL
indexeddblegacy.dll	10.0.19041.488	"IndexedDbLegacy.DYNLINK"
inetcomm.dll	10.0.19041.1	Microsoft Internet Messaging API Resources
inetmib1.dll	10.0.19041.1	Microsoft MIB-II subagent
inetres.dll	10.0.19041.1	Microsoft Internet Messaging API Resources
inked.dll	10.0.19041.329	Microsoft Tablet PC InkEdit Control
inkobjcore.dll	10.0.19041.329	Microsoft Tablet PC Ink Platform Component
input.dll	10.0.19041.1	InputSetting DLL
inputhost.dll	10.0.19041.388	InputHost
inputinjectionbroker.dll	10.0.19041.1	Broker for WinRT input injection.
inputswitch.dll	10.0.19041.488	Microsoft Windows Input Switcher
inseng.dll	11.0.19041.1	Install engine
installservice.dll	10.0.19041.508	InstallService
installservicetasks.dll	10.0.19041.508	InstallService Tasks
intel_opencl_icd32.dll	1.2.11.0	OpenCL Client DLL
intelopencl32.dll	10.18.10.5129	Intel(R) OpenCL(TM) Common Runtime Driver
iologmsg.dll	10.0.19041.1	IO Logging DLL

ipeloggingdictationhelper.dll	1.0.0.1	IPE Logging Library Helper
iphlpapi.dll	10.0.19041.488	IP Helper API
ipnathlpclient.dll	10.0.19041.1	IP NAT Helper Client
iprop.dll	10.0.19041.1	OLE PropertySet Implementation
iprtprio.dll	10.0.19041.450	IP Routing Protocol Priority DLL
iprtrmgr.dll	10.0.19041.450	IP Router Manager
ipsecsnp.dll	10.0.19041.1	IP Security Policy Management Snap-in
ipsmsnap.dll	10.0.19041.1	IP Security Monitor Snap-in
ir32_32.dll	10.0.19041.1	IR32_32 WRAPPER DLL
ir32_32original.dll	3.24.15.3	Intel Indeo(R) Video R3.2 32-bit Driver
ir41_32original.dll	4.51.16.3	Intel Indeo® Video 4.5
ir41_qc.dll	10.0.19041.1	IR41_QC WRAPPER DLL
ir41_qcoriginal.dll	4.30.62.2	Intel Indeo® Video Interactive Quick Compressor
ir41_qcx.dll	10.0.19041.1	IR41_QCX WRAPPER DLL
ir41_qcxoriginal.dll	4.30.64.1	Intel Indeo® Video Interactive Quick Compressor
ir50_32.dll	10.0.19041.1	IR50_32 WRAPPER DLL
ir50_32original.dll	5.2562.15.55	Intel Indeo® video 5.10
ir50_qc.dll	10.0.19041.1	IR50_QC WRAPPER DLL
ir50_qcoriginal.dll	5.0.63.48	Intel Indeo® video 5.10 Quick Compressor
ir50_qcx.dll	10.0.19041.1	IR50_QCX WRAPPER DLL
ir50_qcxoriginal.dll	5.0.64.48	Intel Indeo® video 5.10 Quick Compressor
iri.dll	10.0.19041.1	iri
iscsicpl.dll	5.2.3790.1830	iSCSI Initiator Control Panel Applet
iscsidsc.dll	10.0.19041.1	iSCSI Discovery api
iscsied.dll	10.0.19041.1	iSCSI Extension DLL
iscsium.dll	10.0.19041.1	iSCSI Discovery api
iscsiwmi.dll	10.0.19041.1	MS iSCSI Initiator WMI Provider
iscsiwmiv2.dll	10.0.19041.1	WMI Provider for iSCSI
itircl.dll	10.0.19041.1	Microsoft® InfoTech IR Local DLL
itss.dll	10.0.19041.1	Microsoft® InfoTech Storage System Library
iyuv_32.dll	10.0.19041.1	Intel Indeo(R) Video YUV Codec
javascriptcollectionagent.dll	11.0.19041.1	JavaScript Performance Collection Agent
joinproviderol.dll	10.0.19041.1	Online Join Provider DLL
joinutil.dll	10.0.19041.1	Join Utility DLL
jpmapcontrol.dll	10.0.19041.264	Jupiter Map Control
jscript.dll	5.812.10240.16384	Microsoft ® JScript
jscript9.dll	11.0.19041.508	Microsoft ® JScript
jscript9diag.dll	11.0.19041.508	Microsoft ® JScript Diagnostics
jsproxy.dll	11.0.19041.508	JScript Proxy Auto-Configuration
kbd101.dll	10.0.19041.388	JP Japanese Keyboard Layout for 101
kbd101a.dll	10.0.19041.1	KO Hangeul Keyboard Layout for 101 (Type A)
kbd101b.dll	10.0.19041.1	KO Hangeul Keyboard Layout for 101(Type B)
kbd101c.dll	10.0.19041.1	KO Hangeul Keyboard Layout for 101(Type C)
kbd103.dll	10.0.19041.1	KO Hangeul Keyboard Layout for 103
kbd106.dll	10.0.19041.388	JP Japanese Keyboard Layout for 106
kbd106n.dll	10.0.19041.388	JP Japanese Keyboard Layout for 106
kbda1.dll	10.0.19041.1	Arabic_English_101 Keyboard Layout
kbda2.dll	10.0.19041.1	Arabic_2 Keyboard Layout
kbda3.dll	10.0.19041.1	Arabic_French_102 Keyboard Layout
kbdadlm.dll	10.0.19041.1	Adlam Keyboard Layout
kbdal.dll	10.0.19041.1	Albania Keyboard Layout
kbdarme.dll	10.0.19041.1	Eastern Armenian Keyboard Layout
kbdarmph.dll	10.0.19041.1	Armenian Phonetic Keyboard Layout
kbdarmty.dll	10.0.19041.1	Armenian Typewriter Keyboard Layout
kbdarmw.dll	10.0.19041.1	Western Armenian Keyboard Layout

Navigation

kbdax2.dll	10.0.19041.1	JP Japanese Keyboard Layout for AX2
kbdaze.dll	10.0.19041.1	Azerbaijan_Cyrillic Keyboard Layout
kbdazel.dll	10.0.19041.1	Azeri-Latin Keyboard Layout
kbdazst.dll	10.0.19041.1	Azerbaijani (Standard) Keyboard Layout
kbdbash.dll	10.0.19041.1	Bashkir Keyboard Layout
kbdbe.dll	10.0.19041.1	Belgian Keyboard Layout
kbdbene.dll	10.0.19041.1	Belgian Dutch Keyboard Layout
kbdbgph.dll	10.0.19041.1	Bulgarian Phonetic Keyboard Layout
kbdbgph1.dll	10.0.19041.1	Bulgarian (Phonetic Traditional) Keyboard Layout
kbdbhc.dll	10.0.19041.1	Bosnian (Cyrillic) Keyboard Layout
kbdblr.dll	10.0.19041.1	Belarusian Keyboard Layout
kbdbr.dll	10.0.19041.1	Brazilian Keyboard Layout
kbdbu.dll	10.0.19041.1	Bulgarian (Typewriter) Keyboard Layout
kbdbug.dll	10.0.19041.1	Buginese Keyboard Layout
kbdbulg.dll	10.0.19041.1	Bulgarian Keyboard Layout
kbdca.dll	10.0.19041.1	Canadian Multilingual Keyboard Layout
kbdcan.dll	10.0.19041.1	Canadian Multilingual Standard Keyboard Layout
kbdcher.dll	10.0.19041.1	Cherokee Nation Keyboard Layout
kbdcherp.dll	10.0.19041.1	Cherokee Phonetic Keyboard Layout
kbdcr.dll	10.0.19041.1	Croatian/Slovenian Keyboard Layout
kbdcz.dll	10.0.19041.1	Czech Keyboard Layout
kbdcz1.dll	10.0.19041.1	Czech_101 Keyboard Layout
kbdcz2.dll	10.0.19041.1	Czech_Programmer's Keyboard Layout
kbdda.dll	10.0.19041.1	Danish Keyboard Layout
kbddiv1.dll	10.0.19041.1	Divehi Phonetic Keyboard Layout
kbddiv2.dll	10.0.19041.1	Divehi Typewriter Keyboard Layout
kbddv.dll	10.0.19041.1	Dvorak US English Keyboard Layout
kbddzo.dll	10.0.19041.1	Dzongkha Keyboard Layout
kbdes.dll	10.0.19041.1	Spanish Alernate Keyboard Layout
kbdest.dll	10.0.19041.1	Estonia Keyboard Layout
kbdfa.dll	10.0.19041.1	Persian Keyboard Layout
kbdfar.dll	10.0.19041.1	Persian Standard Keyboard Layout
kbdfc.dll	10.0.19041.1	Canadian French Keyboard Layout
kbdfi.dll	10.0.19041.1	Finnish Keyboard Layout
kbdfi1.dll	10.0.19041.1	Finnish-Swedish with Sami Keyboard Layout
kbdfo.dll	10.0.19041.1	Færoese Keyboard Layout
kbdfr.dll	10.0.19041.1	French Keyboard Layout
kbdfthrk.dll	10.0.19041.1	Futhark Keyboard Layout
kbdgae.dll	10.0.19041.1	Scottish Gaelic (United Kingdom) Keyboard Layout
kbdgeo.dll	10.0.19041.1	Georgian Keyboard Layout
kbdgeoer.dll	10.0.19041.1	Georgian (Ergonomic) Keyboard Layout
kbdgeome.dll	10.0.19041.1	Georgian (MES) Keyboard Layout
kbdgeooa.dll	10.0.19041.1	Georgian (Old Alphabets) Keyboard Layout
kbdgeoqw.dll	10.0.19041.1	Georgian (QWERTY) Keyboard Layout
kbdgkl.dll	10.0.19041.1	Greek_Latin Keyboard Layout
kbdgn.dll	10.0.19041.1	Guarani Keyboard Layout
kbdgr.dll	10.0.19041.1	German Keyboard Layout
kbdgr1.dll	10.0.19041.1	German_IBM Keyboard Layout
kbdgrlnd.dll	10.0.19041.1	Greenlandic Keyboard Layout
kbdgthc.dll	10.0.19041.1	Gothic Keyboard Layout
kbdhau.dll	10.0.19041.1	Hausa Keyboard Layout
kbdhaw.dll	10.0.19041.1	Hawaiian Keyboard Layout
kbdhe.dll	10.0.19041.1	Greek Keyboard Layout
kbdhe220.dll	10.0.19041.1	Greek IBM 220 Keyboard Layout
kbdhe319.dll	10.0.19041.1	Greek IBM 319 Keyboard Layout

Navigation

Navigation

kbdheb.dll	10.0.19041.1	KBDHEB Keyboard Layout
kbdhebl3.dll	10.0.19041.1	Hebrew Standard Keyboard Layout
kbdhela2.dll	10.0.19041.1	Greek IBM 220 Latin Keyboard Layout
kbdhela3.dll	10.0.19041.1	Greek IBM 319 Latin Keyboard Layout
kbdhept.dll	10.0.19041.1	Greek_Polytonic Keyboard Layout
kbdhu.dll	10.0.19041.1	Hungarian Keyboard Layout
kbdhu1.dll	10.0.19041.1	Hungarian 101-key Keyboard Layout
kbdibm02.dll	10.0.19041.1	JP Japanese Keyboard Layout for IBM 5576-002/003
kbdibo.dll	10.0.19041.1	Igbo Keyboard Layout
kbdic.dll	10.0.19041.1	Icelandic Keyboard Layout
kbdinasa.dll	10.0.19041.1	Assamese (Inscript) Keyboard Layout
kbdinbe1.dll	10.0.19041.1	Bengali - Inscript (Legacy) Keyboard Layout
kbdinbe2.dll	10.0.19041.1	Bengali (Inscript) Keyboard Layout
kbdinben.dll	10.0.19041.1	Bengali Keyboard Layout
kbdindev.dll	10.0.19041.1	Devanagari Keyboard Layout
kbdinen.dll	10.0.19041.1	English (India) Keyboard Layout
kbdinguj.dll	10.0.19041.1	Gujarati Keyboard Layout
kbdinhin.dll	10.0.19041.1	Hindi Keyboard Layout
kbdinkan.dll	10.0.19041.1	Kannada Keyboard Layout
kbdinmal.dll	10.0.19041.1	Malayalam Keyboard Layout Keyboard Layout
kbdinmar.dll	10.0.19041.1	Marathi Keyboard Layout
kbdinori.dll	10.0.19041.1	Odia Keyboard Layout
kbdinpun.dll	10.0.19041.1	Punjabi/Gurmukhi Keyboard Layout
kbdintam.dll	10.0.19041.1	Tamil Keyboard Layout
kbdintel.dll	10.0.19041.1	Telugu Keyboard Layout
kbdinuk2.dll	10.0.19041.1	Inuktitut Naqittaut Keyboard Layout
kbdir.dll	10.0.19041.1	Irish Keyboard Layout
kbdit.dll	10.0.19041.1	Italian Keyboard Layout
kbdit142.dll	10.0.19041.1	Italian 142 Keyboard Layout
kbdiulat.dll	10.0.19041.1	Inuktitut Latin Keyboard Layout
kbdjav.dll	10.0.19041.1	Javanese Keyboard Layout
kbdjpn.dll	10.0.19041.388	JP Japanese Keyboard Layout Stub driver
kbdkaz.dll	10.0.19041.1	Kazak_Cyrillic Keyboard Layout
kbdkhmr.dll	10.0.19041.1	Cambodian Standard Keyboard Layout
kbdkni.dll	10.0.19041.1	Khmer (NIDA) Keyboard Layout
kbdkor.dll	10.0.19041.1	KO Hangeul Keyboard Layout Stub driver
kbdkurd.dll	10.0.19041.1	Central Kurdish Keyboard Layout
kbdkyr.dll	10.0.19041.1	Kyrgyz Keyboard Layout
kbdla.dll	10.0.19041.1	Latin-American Spanish Keyboard Layout
kbdlao.dll	10.0.19041.1	Lao Standard Keyboard Layout
kbdlisub.dll	10.0.19041.1	Lisu Basic Keyboard Layout
kbdlisus.dll	10.0.19041.1	Lisu Standard Keyboard Layout
kbdlk41a.dll	10.0.19041.1	DEC LK411-AJ Keyboard Layout
kbdlt.dll	10.0.19041.1	Lithuania Keyboard Layout
kbdlt1.dll	10.0.19041.1	Lithuanian Keyboard Layout
kbdlt2.dll	10.0.19041.1	Lithuanian Standard Keyboard Layout
kbdlv.dll	10.0.19041.1	Latvia Keyboard Layout
kbdlv1.dll	10.0.19041.1	Latvia-QWERTY Keyboard Layout
kbdlvst.dll	10.0.19041.1	Latvian (Standard) Keyboard Layout
kbdmac.dll	10.0.19041.1	Macedonian (North Macedonia) Keyboard Layout
kbdmacst.dll	10.0.19041.1	Macedonian (North Macedonia) - Standard Keyboard Layout
kbdmaori.dll	10.0.19041.1	Maori Keyboard Layout
kbdmlt47.dll	10.0.19041.1	Maltese 47-key Keyboard Layout
kbdmlt48.dll	10.0.19041.1	Maltese 48-key Keyboard Layout
kbdmon.dll	10.0.19041.1	Mongolian Keyboard Layout

kbdmonmo.dll	10.0.19041.1	Mongolian (Mongolian Script) Keyboard Layout
kbdmonst.dll	10.0.19041.1	Traditional Mongolian (Standard) Keyboard Layou
kbdmyan.dll	10.0.19041.1	Myanmar Keyboard Layout
kbdne.dll	10.0.19041.1	Dutch Keyboard Layout
kbdnec.dll	10.0.19041.1	JP Japanese Keyboard Layout for (NEC PC-9800)
kbdnec95.dll	10.0.19041.1	JP Japanese Keyboard Layout for (NEC PC-9800 Windows 95)
kbdnecat.dll	10.0.19041.1	JP Japanese Keyboard Layout for (NEC PC-9800 on PC98-NX)
kbdnecnt.dll	10.0.19041.1	JP Japanese NEC PC-9800 Keyboard Layout
kbdnepr.dll	10.0.19041.1	Nepali Keyboard Layout
kbdnko.dll	10.0.19041.1	N'Ko Keyboard Layout
kbdno.dll	10.0.19041.1	Norwegian Keyboard Layout
kbdno1.dll	10.0.19041.1	Norwegian with Sami Keyboard Layout
kbdnso.dll	10.0.19041.1	Sesotho sa Leboa Keyboard Layout
kbdntl.dll	10.0.19041.1	New Tai Leu Keyboard Layout
kbdogham.dll	10.0.19041.1	Ogham Keyboard Layout
kbdolch.dll	10.0.19041.1	Ol Chiki Keyboard Layout
kbdoldit.dll	10.0.19041.1	Old Italic Keyboard Layout
kbdosa.dll	10.0.19041.1	Osage Keyboard Layout
kbdosm.dll	10.0.19041.1	Osmanya Keyboard Layout
kbdpash.dll	10.0.19041.1	Pashto (Afghanistan) Keyboard Layout
kbdphags.dll	10.0.19041.1	Phags-pa Keyboard Layout
kbdpl.dll	10.0.19041.1	Polish Keyboard Layout
kbdpl1.dll	10.0.19041.1	Polish Programmer's Keyboard Layout
kbdpo.dll	10.0.19041.1	Portuguese Keyboard Layout
kbdro.dll	10.0.19041.1	Romanian (Legacy) Keyboard Layout
kbdropr.dll	10.0.19041.1	Romanian (Programmers) Keyboard Layout
kbdrost.dll	10.0.19041.1	Romanian (Standard) Keyboard Layout
kbdru.dll	10.0.19041.1	Russian Keyboard Layout
kbdru1.dll	10.0.19041.1	Russia(Typewriter) Keyboard Layout
kbdrum.dll	10.0.19041.1	Russian - Mnemonic Keyboard Layout
kbdsf.dll	10.0.19041.1	Swiss French Keyboard Layout
kbdsg.dll	10.0.19041.1	Swiss German Keyboard Layout
kbdsl.dll	10.0.19041.1	Slovak Keyboard Layout
kbdsl1.dll	10.0.19041.1	Slovak(QWERTY) Keyboard Layout
kbdsmsfi.dll	10.0.19041.1	Sami Extended Finland-Sweden Keyboard Layout
kbdsmsno.dll	10.0.19041.1	Sami Extended Norway Keyboard Layout
kbdsn1.dll	10.0.19041.1	Sinhala Keyboard Layout
kbdsora.dll	10.0.19041.1	Sora Keyboard Layout
kbdsorex.dll	10.0.19041.1	Sorbian Extended Keyboard Layout
kbdsors1.dll	10.0.19041.1	Sorbian Standard Keyboard Layout
kbdsorst.dll	10.0.19041.1	Sorbian Standard (Legacy) Keyboard Layout
kbdsp.dll	10.0.19041.1	Spanish Keyboard Layout
kbdsw.dll	10.0.19041.1	Swedish Keyboard Layout
kbdsw09.dll	10.0.19041.1	Sinhala - Wij 9 Keyboard Layout
kbdsyr1.dll	10.0.19041.1	Syriac Standard Keyboard Layout
kbdsyr2.dll	10.0.19041.1	Syriac Phoenetic Keyboard Layout
kbdtaile.dll	10.0.19041.1	Tai Le Keyboard Layout
kbdtajik.dll	10.0.19041.1	Tajik Keyboard Layout
kbdtat.dll	10.0.19041.1	Tatar (Legacy) Keyboard Layout
kbdth0.dll	10.0.19041.1	Thai Kedmanee Keyboard Layout
kbdth1.dll	10.0.19041.1	Thai Pattachote Keyboard Layout
kbdth2.dll	10.0.19041.1	Thai Kedmanee (non-ShiftLock) Keyboard Layout
kbdth3.dll	10.0.19041.1	Thai Pattachote (non-ShiftLock) Keyboard Layout
kbdtifi.dll	10.0.19041.1	Tifinagh (Basic) Keyboard Layout
kbdtifi2.dll	10.0.19041.1	Tifinagh (Extended) Keyboard Layout

Navigation

Navigation

kbdtiprc.dll	10.0.19041.1	Tibetan (PRC) Keyboard Layout
kbdtiprd.dll	10.0.19041.1	Tibetan (PRC) - Updated Keyboard Layout
kbdtt102.dll	10.0.19041.1	Tatar Keyboard Layout
kbdtuf.dll	10.0.19041.1	Turkish F Keyboard Layout
kbdtuq.dll	10.0.19041.1	Turkish Q Keyboard Layout
kbdturme.dll	10.0.19041.1	Turkmen Keyboard Layout
kbdtzm.dll	10.0.19041.1	Central Atlas Tamazight Keyboard Layout
kbdughr.dll	10.0.19041.1	Uyghur (Legacy) Keyboard Layout
kbdughr1.dll	10.0.19041.1	Uyghur Keyboard Layout
kbduk.dll	10.0.19041.1	United Kingdom Keyboard Layout
kbdukx.dll	10.0.19041.1	United Kingdom Extended Keyboard Layout
kbdur.dll	10.0.19041.1	Ukrainian Keyboard Layout
kbdur1.dll	10.0.19041.1	Ukrainian (Enhanced) Keyboard Layout
kbdurdu.dll	10.0.19041.1	Urdu Keyboard Layout
kbdus.dll	10.0.19041.1	United States Keyboard Layout
kbdusa.dll	10.0.19041.1	US IBM Arabic 238_L Keyboard Layout
kbdusl.dll	10.0.19041.1	Dvorak Left-Hand US English Keyboard Layout
kbdusr.dll	10.0.19041.1	Dvorak Right-Hand US English Keyboard Layout
kbdusx.dll	10.0.19041.1	US Multinational Keyboard Layout
kbduzb.dll	10.0.19041.1	Uzbek_Cyrillic Keyboard Layout
kbdvntc.dll	10.0.19041.1	Vietnamese Keyboard Layout
kbdwol.dll	10.0.19041.1	Wolof Keyboard Layout
kbdyak.dll	10.0.19041.1	Sakha - Russia Keyboard Layout
kbdyba.dll	10.0.19041.1	Yoruba Keyboard Layout
kbdycc.dll	10.0.19041.1	Serbian (Cyrillic) Keyboard Layout
kbdycl.dll	10.0.19041.1	Serbian (Latin) Keyboard Layout
kerbclientshared.dll	10.0.19041.488	Kerberos Client Shared Functionality
kerberos.dll	10.0.19041.488	Kerberos Security Package
kernel.appcore.dll	10.0.19041.1	AppModel API Host
kernel32.dll	10.0.19041.292	Windows NT BASE API Client DLL
kernelbase.dll	10.0.19041.488	Windows NT BASE API Client DLL
keycredmgr.dll	10.0.19041.1	Microsoft Key Credential Manager
keyiso.dll	10.0.19041.388	CNG Key Isolation Service
keymgr.dll	10.0.19041.1	Stored User Names and Passwords
ksuser.dll	10.0.19041.1	User CSA Library
ktmw32.dll	10.0.19041.1	Windows KTM Win32 Client DLL
l2gpstore.dll	10.0.19041.1	Policy Storage dll
l2nacp.dll	10.0.19041.1	Windows Onex Credential Provider
l2sechc.dll	10.0.19041.1	Layer 2 Security Diagnostics Helper Classes
languageoverlayutil.dll	10.0.19041.1	Provides helper APIs for managing overlaid localized Windows resources.
laprxy.dll	12.0.19041.1	Windows Media Logagent Proxy
licensemanager.dll	10.0.19041.173	LicenseManager
licensemanagerapi.dll	10.0.19041.173	"LicenseManagerApi.DYNLINK"
licensingdiagspp.dll	10.0.19041.1	Licensing Diagnostics SPP Plugin
licensingwinrt.dll	10.0.19041.488	LicensingWinRuntime
licmgr10.dll	11.0.19041.1	Microsoft® License Manager DLL
linkinfo.dll	10.0.19041.1	Windows Volume Tracking
loadperf.dll	10.0.19041.1	Load & Unload Performance Counters
localsec.dll	10.0.19041.1	Local Users and Groups MMC Snapin
locationapi.dll	10.0.19041.329	Microsoft Windows Location API
locationframeworkinternalps.dll	10.0.19041.1	Windows Geolocation Framework Internal PS
locationframeworkps.dll	10.0.19041.1	Windows Geolocation Framework PS
lockappbroker.dll	10.0.19041.388	Windows Lock App Broker DLL
lockscreendata.dll	10.0.19041.1	Windows Lock Screen Data DLL
loghours.dll	10.0.19041.1	Schedule Dialog

Navigation

logoncli.dll	10.0.19041.388	Net Logon Client DLL
lpk.dll	10.0.19041.508	Language Pack
lsmproxy.dll	10.0.19041.1	LSM interfaces proxy Dll
luainstall.dll	10.0.19041.1	Lua manifest install
luiapi.dll	10.0.19041.1	LUI API
lz32.dll	5.0.1.1	LZ Expand/Compress API DLL
magnification.dll	10.0.19041.1	Microsoft Magnification API
mapconfiguration.dll	10.0.19041.1	MapConfiguration
mapcontrolcore.dll	10.0.19041.1	Map Control Core
mapcontrolstringsres.dll	10.0.19041.1	Map control resource strings
mapgeocoder.dll	10.0.19041.264	Maps Geocoder
mapi32.dll	1.0.2536.0	Extended MAPI 1.0 for Windows NT
mapistub.dll	1.0.2536.0	Extended MAPI 1.0 for Windows NT
maprouter.dll	10.0.19041.488	Maps Router
mapsbtsvc.dll	10.0.19041.1	Maps Background Transfer Service
mbaeapi.dll	10.0.19041.117	Mobile Broadband Account Experience API
mbaeapipublic.dll	10.0.19041.423	Mobile Broadband Account API
mbsmsapi.dll	10.0.19041.264	Microsoft Windows Mobile Broadband SMS API
mbussdapi.dll	10.0.19041.264	Microsoft Windows Mobile Broadband USSD API
mccsengineshared.dll	10.0.19041.1	Utilies shared among OneSync engines
mciavi32.dll	10.0.19041.1	Video For Windows MCI driver
mcicda.dll	10.0.19041.1	MCI driver for cdaudio devices
mciqtz32.dll	10.0.19041.1	DirectShow MCI Driver
mciseq.dll	10.0.19041.1	MCI driver for MIDI sequencer
mciwave.dll	10.0.19041.1	MCI driver for waveform audio
mcrecvsrc.dll	10.0.19041.153	Miracast Media Foundation Source DLL
mdminst.dll	10.0.19041.1	Modem Class Installer
mdmlocalmanagement.dll	10.0.19041.423	MDM Local Management DLL
mdmregistration.dll	10.0.19041.488	MDM Registration DLL
messagingdatamodel2.dll	10.0.19041.1	MessagingDataModel2
mf.dll	10.0.19041.488	Media Foundation DLL
mf3216.dll	10.0.19041.508	32-bit to 16-bit Metafile Conversion DLL
mfaacenc.dll	10.0.19041.1	Media Foundation AAC Encoder
mfasfsrcsnk.dll	10.0.19041.488	Media Foundation ASF Source and Sink DLL
mfaudiocnv.dll	10.0.19041.1	Media Foundation Audio Converter DLL
mfc100.dll	10.0.40219.325	MFCDLL Shared Library - Retail Version
mfc100chs.dll	10.0.40219.325	MFC Language Specific Resources
mfc100cht.dll	10.0.40219.325	MFC Language Specific Resources
mfc100deu.dll	10.0.40219.325	MFC Language Specific Resources
mfc100enu.dll	10.0.40219.325	MFC Language Specific Resources
mfc100esn.dll	10.0.40219.325	MFC Language Specific Resources
mfc100fra.dll	10.0.40219.325	MFC Language Specific Resources
mfc100ita.dll	10.0.40219.325	MFC Language Specific Resources
mfc100jpn.dll	10.0.40219.325	MFC Language Specific Resources
mfc100kor.dll	10.0.40219.325	MFC Language Specific Resources
mfc100rus.dll	10.0.40219.325	MFC Language Specific Resources
mfc100u.dll	10.0.40219.325	MFCDLL Shared Library - Retail Version
mfc110.dll	11.0.60610.1	MFCDLL Shared Library - Retail Version
mfc110chs.dll	11.0.60610.1	MFC Language Specific Resources
mfc110cht.dll	11.0.60610.1	MFC Language Specific Resources
mfc110deu.dll	11.0.60610.1	MFC Language Specific Resources
mfc110enu.dll	11.0.60610.1	MFC Language Specific Resources
mfc110esn.dll	11.0.60610.1	MFC Language Specific Resources
mfc110fra.dll	11.0.60610.1	MFC Language Specific Resources
mfc110ita.dll	11.0.60610.1	MFC Language Specific Resources

Navigation

mfc110jpn.dll	11.0.60610.1	MFC Language Specific Resources
mfc110kor.dll	11.0.60610.1	MFC Language Specific Resources
mfc110rus.dll	11.0.60610.1	MFC Language Specific Resources
mfc110u.dll	11.0.60610.1	MFCDLL Shared Library - Retail Version
mfc120.dll	12.0.40660.0	MFCDLL Shared Library - Retail Version
mfc120chs.dll	12.0.40660.0	MFC Language Specific Resources
mfc120cht.dll	12.0.40660.0	MFC Language Specific Resources
mfc120deu.dll	12.0.40660.0	MFC Language Specific Resources
mfc120enu.dll	12.0.40660.0	MFC Language Specific Resources
mfc120esn.dll	12.0.40660.0	MFC Language Specific Resources
mfc120fra.dll	12.0.40660.0	MFC Language Specific Resources
mfc120ita.dll	12.0.40660.0	MFC Language Specific Resources
mfc120jpn.dll	12.0.40660.0	MFC Language Specific Resources
mfc120kor.dll	12.0.40660.0	MFC Language Specific Resources
mfc120rus.dll	12.0.40660.0	MFC Language Specific Resources
mfc120u.dll	12.0.40660.0	MFCDLL Shared Library - Retail Version
mfc140.dll	14.24.28127.4	MFCDLL Shared Library - Retail Version
mfc140chs.dll	14.24.28127.4	MFC Language Specific Resources
mfc140cht.dll	14.24.28127.4	MFC Language Specific Resources
mfc140deu.dll	14.24.28127.4	MFC Language Specific Resources
mfc140enu.dll	14.24.28127.4	MFC Language Specific Resources
mfc140esn.dll	14.24.28127.4	MFC Language Specific Resources
mfc140fra.dll	14.24.28127.4	MFC Language Specific Resources
mfc140ita.dll	14.24.28127.4	MFC Language Specific Resources
mfc140jpn.dll	14.24.28127.4	MFC Language Specific Resources
mfc140kor.dll	14.24.28127.4	MFC Language Specific Resources
mfc140rus.dll	14.24.28127.4	MFC Language Specific Resources
mfc140u.dll	14.24.28127.4	MFCDLL Shared Library - Retail Version
mfc40.dll	4.1.0.6140	MFCDLL Shared Library - Retail Version
mfc40u.dll	4.1.0.6140	MFCDLL Shared Library - Retail Version
mfc42.dll	6.6.8063.0	MFCDLL Shared Library - Retail Version
mfc42u.dll	6.6.8063.0	MFCDLL Shared Library - Retail Version
mfcaptureengine.dll	10.0.19041.329	Media Foundation CaptureEngine DLL
mfcm100.dll	10.0.40219.325	MFC Managed Library - Retail Version
mfcm100u.dll	10.0.40219.325	MFC Managed Library - Retail Version
mfcm110.dll	11.0.60610.1	MFC Managed Library - Retail Version
mfcm110u.dll	11.0.60610.1	MFC Managed Library - Retail Version
mfcm120.dll	12.0.40660.0	MFC Managed Library - Retail Version
mfcm120u.dll	12.0.40660.0	MFC Managed Library - Retail Version
mfcm140.dll	14.24.28127.4	MFC Managed Library - Retail Version
mfcm140u.dll	14.24.28127.4	MFC Managed Library - Retail Version
mfcore.dll	10.0.19041.488	Media Foundation Core DLL
mfcsubs.dll	2001.12.10941.16384	COM+
mfds.dll	10.0.19041.508	Media Foundation Direct Show wrapper DLL
mfdvdec.dll	10.0.19041.1	Media Foundation DV Decoder
mferror.dll	10.0.19041.1	Media Foundation Error DLL
mfh263enc.dll	10.0.19041.1	Media Foundation h263 Encoder
mfh264enc.dll	10.0.19041.1	Media Foundation H264 Encoder
mfksproxy.dll	10.0.19041.1	Dshow MF Bridge DLL DLL
mfmediaengine.dll	10.0.19041.488	Media Foundation Media Engine DLL
mfmjpegdec.dll	10.0.19041.329	Media Foundation MJPEG Decoder
mfmkvsrcsnk.dll	10.0.19041.207	Media Foundation MKV Media Source and Sink DLL
mfmp4srcsnk.dll	10.0.19041.450	Media Foundation MPEG4 Source and Sink DLL
mfmpeg2srcsnk.dll	10.0.19041.488	Media Foundation MPEG2 Source and Sink DLL
mfnetcore.dll	10.0.19041.423	Media Foundation Net Core DLL

Navigation

mfnetsrc.dll	10.0.19041.423	Media Foundation Net Source DLL
mfperfhelper.dll	10.0.19041.1	MFPerf DLL
mfplat.dll	10.0.19041.488	Media Foundation Platform DLL
mfplay.dll	10.0.19041.1	Media Foundation Playback API DLL
mfps.dll	10.0.19041.1	Media Foundation Proxy DLL
mfreadwrite.dll	10.0.19041.153	Media Foundation ReadWrite DLL
mfsensorgroup.dll	10.0.19041.423	Media Foundation Sensor Group DLL
mfsrcsnk.dll	10.0.19041.264	Media Foundation Source and Sink DLL
mfsvr.dll	10.0.19041.488	Media Foundation Simple Video Renderer DLL
mftranscode.dll	10.0.19041.1	Media Foundation Transcode DLL
mfvdsp.dll	10.0.19041.1	Windows Media Foundation Video DSP Components
mfvfw.dll	10.0.19041.1	MF VFW MFT
mfwmaaec.dll	10.0.19041.1	Windows Media Audio AEC for Media Foundation
mgmtapi.dll	10.0.19041.1	Microsoft SNMP Manager API (uses WinSNMP)
mi.dll	10.0.19041.1	Management Infrastructure
mibincodec.dll	10.0.19041.1	Management Infrastructure binary codec component
microsoft.bluetooth.proxy.dll	10.0.19041.1	Microsoft Bluetooth COM Proxy DLL
microsoft.management.infrastructure.native.unmanaged.dll	10.0.19041.1	Microsoft.Management.Infrastructure.Native.Unmanaged.dll
microsoft.uev.appagent.dll	10.0.19041.488	Microsoft.Uev.AppAgent DLL
microsoft.uev.office2010customactions.dll	10.0.19041.488	Microsoft.Uev.Office2010CustomActions DLL
microsoft.uev.office2013customactions.dll	10.0.19041.488	Microsoft.Uev.Office2013CustomActions DLL
microsoftaccounttokenprovider.dll	10.0.19041.423	Microsoft® Account Token Provider
microsoftaccountwamextension.dll	10.0.19041.488	Microsoft Account WAM Extension DLL
midimap.dll	10.0.19041.488	Microsoft MIDI Mapper
migisol.dll	10.0.19041.1	Migration System Isolation Layer
miguiresource.dll	10.0.19041.1	MIG wini32 resources
mimefilt.dll	2008.0.19041.1	MIME Filter
mimofcodec.dll	10.0.19041.1	Management Infrastructure mof codec component
minstoreevents.dll	10.0.19041.1	Minstore Event Resource
miracastreceiver.dll	10.0.19041.488	Miracast Receiver API
miracastreceiverext.dll	10.0.19041.388	Miracast Receiver Extensions
mirrordrvcompat.dll	10.0.19041.1	Mirror Driver Compatibility Helper
mispace.dll	10.0.19041.1	Storage Management Provider for Spaces
mitigationconfiguration.dll	10.0.19041.1	Exploit Guard Configuration Helper
miutils.dll	10.0.19041.1	Management Infrastructure
mixedrealityruntime.dll	10.0.19041.1	MixedRealityRuntime DLL
mlang.dll	10.0.19041.1	Multi Language Support DLL
mls3.dll	10.0.19041.1	Microsoft Neutral Natural Language Server Data and Code
mmcbase.dll	10.0.19041.1	MMC Base DLL
mmcndmgr.dll	10.0.19041.329	MMC Node Manager DLL
mmcshext.dll	10.0.19041.1	MMC Shell Extension DLL
mmdevapi.dll	10.0.19041.488	MMDevice API
mmgaclient.dll	10.0.19041.1	MMGA
mmgaproxystub.dll	10.0.19041.1	MMGA
mmres.dll	10.0.19041.1	General Audio Resources
mobilenetworking.dll	10.0.19041.1	"MobileNetworking.DYNLINK"
modemui.dll	10.0.19041.1	Windows Modem Properties
moricons.dll	10.0.19041.1	Windows NT Setup Icon Resources Library
moshostclient.dll	10.0.19041.1	MosHostClient
mosstorage.dll	10.0.19041.1	MosStorage
mp3dmod.dll	10.0.19041.1	Microsoft MP3 Decoder DMO
mp43decd.dll	10.0.19041.1	Windows Media MPEG-4 Video Decoder
mp4sdecd.dll	10.0.19041.450	Windows Media MPEG-4 S Video Decoder
mpg4decd.dll	10.0.19041.1	Windows Media MPEG-4 Video Decoder
mpr.dll	10.0.19041.1	Multiple Provider Router DLL

mprapi.dll	10.0.19041.1	Windows NT MP Router Administration DLL
mprddm.dll	10.0.19041.1	Demand Dial Manager Supervisor
mprdim.dll	10.0.19041.450	Dynamic Interface Manager
mprext.dll	10.0.19041.1	Multiple Provider Router Extension DLL
mprmsg.dll	10.0.19041.1	Multi-Protocol Router Service Messages DLL
mrmcorer.dll	10.0.19041.388	Microsoft Windows MRM
mrmdeploy.dll	10.0.19041.1	Microsoft Windows MRM Deployment
mrmindexer.dll	10.0.19041.264	Microsoft Windows MRM
mrt_map.dll	1.6.24911.0	Microsoft .NET Native Error Reporting Helper
mrt100.dll	1.6.24911.0	Microsoft .NET Native Runtime
ms3dthumbnailprovider.dll	10.0.19041.1	3D Builder
msaatext.dll	2.0.10413.0	Active Accessibility text support
msac3enc.dll	10.0.19041.1	Microsoft AC-3 Encoder
msacm32.dll	10.0.19041.1	Microsoft ACM Audio Filter
msadce.dll	10.0.19041.329	OLE DB Cursor Engine
msadce.dll	10.0.19041.329	OLE DB Cursor Engine
msadcer.dll	10.0.19041.1	OLE DB Cursor Engine Resources
msadcer.dll	10.0.19041.1	OLE DB Cursor Engine Resources
msadco.dll	10.0.19041.329	Remote Data Services Data Control
msadco.dll	10.0.19041.329	Remote Data Services Data Control
msadcor.dll	10.0.19041.1	Remote Data Services Data Control Resources
msadcor.dll	10.0.19041.1	Remote Data Services Data Control Resources
msadds.dll	10.0.19041.1	OLE DB Data Shape Provider
msadds.dll	10.0.19041.1	OLE DB Data Shape Provider
msaddsr.dll	10.0.19041.1	OLE DB Data Shape Provider Resources
msaddsr.dll	10.0.19041.1	OLE DB Data Shape Provider Resources
msader15.dll	10.0.19041.1	ActiveX Data Objects Resources
msader15.dll	10.0.19041.1	ActiveX Data Objects Resources
msado15.dll	10.0.19041.329	ActiveX Data Objects
msado15.dll	10.0.19041.329	ActiveX Data Objects
msadomd.dll	10.0.19041.264	ActiveX Data Objects (Multi-Dimensional)
msadomd.dll	10.0.19041.264	ActiveX Data Objects (Multi-Dimensional)
msador15.dll	10.0.19041.1	Microsoft ActiveX Data Objects Recordset
msador15.dll	10.0.19041.1	Microsoft ActiveX Data Objects Recordset
msadox.dll	10.0.19041.264	ActiveX Data Objects Extensions
msadox.dll	10.0.19041.264	ActiveX Data Objects Extensions
msadrh15.dll	10.0.19041.1	ActiveX Data Objects Rowset Helper
msadrh15.dll	10.0.19041.1	ActiveX Data Objects Rowset Helper
msafd.dll	10.0.19041.1	Microsoft Windows Sockets 2.0 Service Provider
msajapi.dll	10.0.19041.1	AllJoyn API Library
msalacdecoder.dll	10.0.19041.1	Media Foundation ALAC Decoder
msalacencoder.dll	10.0.19041.1	Media Foundation ALAC Encoder
msamrnbdecoder.dll	10.0.19041.1	AMR Narrowband Decoder DLL
msamrnbencoder.dll	10.0.19041.1	AMR Narrowband Encoder DLL
msamrnbsink.dll	10.0.19041.1	AMR Narrowband Sink DLL
msamrnbsource.dll	10.0.19041.1	AMR Narrowband Source DLL
msasn1.dll	10.0.19041.1	ASN.1 Runtime APIs
msauddecmft.dll	10.0.19041.388	Media Foundation Audio Decoders
msaudite.dll	10.0.19041.1	Security Audit Events DLL
msauserext.dll	10.0.19041.423	MSA USER Extension DLL
mscandui.dll	10.0.19041.1	MSCANDUI Server DLL
mscat32.dll	10.0.19041.1	MSCAT32 Forwarder DLL
msclmd.dll	10.0.19041.1	Microsoft Class Mini-driver
mscms.dll	10.0.19041.264	Microsoft Color Matching System DLL
mscoree.dll	10.0.19041.1	Microsoft .NET Runtime Execution Engine

Navigation

mscorier.dll	10.0.19041.1	Microsoft .NET Runtime IE resources
mscories.dll	2.0.50727.9149	Microsoft .NET IE SECURITY REGISTRATION
mscpx32r.dll	10.0.19041.1	ODBC Code Page Translator Resources
mscpxl32.dll	10.0.19041.1	ODBC Code Page Translator
msctf.dll	10.0.19041.488	MSCTF Server DLL
msctfmonitor.dll	10.0.19041.1	MsCtfMonitor DLL
msctfp.dll	10.0.19041.1	MSCTFP Server DLL
msctfui.dll	10.0.19041.1	MSCTFUI Server DLL
msctfuimanager.dll	10.0.19041.1	Microsoft UIManager DLL
msdadc.dll	10.0.19041.1	OLE DB Data Conversion Stub
msdadiag.dll	10.0.19041.1	Built-In Diagnostics
msdaenum.dll	10.0.19041.1	OLE DB Root Enumerator Stub
msdaer.dll	10.0.19041.1	OLE DB Error Collection Stub
msdaora.dll	10.0.19041.329	OLE DB Provider for Oracle
msdaorar.dll	10.0.19041.1	OLE DB Provider for Oracle Resources
msdaosp.dll	10.0.19041.1	OLE DB Simple Provider
msdaosp.dll	10.0.19041.1	OLE DB Simple Provider
msdaprsr.dll	10.0.19041.1	OLE DB Persistence Services Resources
msdaprsr.dll	10.0.19041.1	OLE DB Persistence Services Resources
msdaprst.dll	10.0.19041.1	OLE DB Persistence Services
msdaprst.dll	10.0.19041.1	OLE DB Persistence Services
msdaps.dll	10.0.19041.1	OLE DB Interface Proxies/Stubs
msdaps.dll	10.0.19041.1	OLE DB Interface Proxies/Stubs
msdarem.dll	10.0.19041.1	OLE DB Remote Provider
msdarem.dll	10.0.19041.1	OLE DB Remote Provider
msdaremr.dll	10.0.19041.1	OLE DB Remote Provider Resources
msdaremr.dll	10.0.19041.1	OLE DB Remote Provider Resources
msdart.dll	10.0.19041.1	OLE DB Runtime Routines
msdasc.dll	10.0.19041.1	OLE DB Service Components Stub
msdasql.dll	10.0.19041.1	OLE DB Provider for ODBC Drivers
msdasql.dll	10.0.19041.1	OLE DB Provider for ODBC Drivers
msdasqlr.dll	10.0.19041.1	OLE DB Provider for ODBC Drivers Resources
msdasqlr.dll	10.0.19041.1	OLE DB Provider for ODBC Drivers Resources
msdatl3.dll	10.0.19041.1	OLE DB Implementation Support Routines
msdatl3.dll	10.0.19041.1	OLE DB Implementation Support Routines
msdatt.dll	10.0.19041.1	OLE DB Temporary Table Services
msdaurl.dll	10.0.19041.1	OLE DB RootBinder Stub
msdelta.dll	5.0.1.1	Microsoft Patch Engine
msdfmap.dll	10.0.19041.1	Data Factory Handler
msdfmap.dll	10.0.19041.1	Data Factory Handler
msdmo.dll	10.0.19041.1	DMO Runtime
msdrm.dll	10.0.19041.1	Windows Rights Management client
msdtcprx.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator OLE Transactions Interface Proxy DLL
msdtcspoffln.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator SysPrep Specialize Offline DLL
msdtcuiu.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator Administrative DLL
msdtcvsp1res.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator Resources for Vista SP1
msexch40.dll	4.0.9756.0	Microsoft Jet Exchange Isam
msexcl40.dll	4.0.9801.21	Microsoft Jet Excel Isam
msfeeds.dll	11.0.19041.1	Microsoft Feeds Manager
msfeedsbs.dll	11.0.19041.1	Microsoft Feeds Background Sync
msflacdecoder.dll	10.0.19041.207	Media Foundation FLAC Decoder
msflacencoder.dll	10.0.19041.153	Media Foundation FLAC Encoder
msftedit.dll	10.0.19041.488	Rich Text Edit Control, v8.5
msheif.dll	10.0.19041.1	HEIF DLL
mshtml.dll	11.0.19041.508	Microsoft (R) HTML Viewer

Navigation

Navigation

mshtmldac.dll	11.0.19041.1	DAC for Trident DOM
mshtmled.dll	11.0.19041.329	Microsoft® HTML Editing Component
mshtmler.dll	11.0.19041.1	Microsoft® HTML Editing Component's Resource DLL
msi.dll	5.0.19041.508	Windows Installer
msidcrl40.dll	10.0.19041.423	Microsoft® Account Dynamic Link Library
msident.dll	10.0.19041.1	Microsoft Identity Manager
msidle.dll	10.0.19041.1	User Idle Monitor
msidntld.dll	10.0.19041.1	Microsoft Identity Manager
msieftp.dll	10.0.19041.1	Microsoft Internet Explorer FTP Folder Shell Extension
msihnd.dll	5.0.19041.1	Windows® installer
msiltcfg.dll	5.0.19041.1	Windows Installer Configuration API Stub
msimg32.dll	10.0.19041.508	GDIEXT Client DLL
msimsg.dll	5.0.19041.508	Windows® Installer International Messages
msimtf.dll	10.0.19041.1	Active IMM Server DLL
msisip.dll	5.0.19041.450	MSI Signature SIP Provider
msiso.dll	11.0.19041.488	Isolation Library for Internet Explorer
msiwer.dll	5.0.19041.1	MSI Windows Error Reporting
msjet40.dll	4.0.9801.27	Microsoft Jet Engine Library
msjetoledb40.dll	4.0.9801.0	
msjint40.dll	4.0.9801.1	Microsoft Jet Database Engine International DLL
msjro.dll	10.0.19041.1	Jet and Replication Objects
msjter40.dll	4.0.9801.0	Microsoft Jet Database Engine Error DLL
msjtes40.dll	4.0.9801.0	Microsoft Jet Expression Service
mskeyprotcli.dll	10.0.19041.423	Windows Client Key Protection Provider
mskeyprotect.dll	10.0.19041.1	Microsoft Key Protection Provider
msls31.dll	3.10.349.0	Microsoft Line Services library file
msltus40.dll	4.0.9801.21	Microsoft Jet Lotus 1-2-3 Isam
msmpeg2adec.dll	10.0.19041.1	Microsoft DTV-DVD Audio Decoder
msmpeg2enc.dll	10.0.19041.1	Microsoft MPEG-2 Encoder
msmpeg2vdec.dll	10.0.19041.488	Microsoft DTV-DVD Video Decoder
msobjs.dll	10.0.19041.1	System object audit names
msoert2.dll	10.0.19041.1	Microsoft Windows Mail RT Lib
msopusdecoder.dll	10.0.19041.1	Media Foundation Opus Decoder
msorc32r.dll	10.0.19041.1	ODBC Driver for Oracle Resources
msorcl32.dll	10.0.19041.1	ODBC Driver for Oracle
mspatcha.dll	5.0.1.1	Microsoft File Patch Application API
mspatchc.dll	5.0.1.1	Microsoft Patch Creation Engine
mspbde40.dll	4.0.9801.15	Microsoft Jet Paradox Isam
msphotography.dll	10.0.19041.264	MS Photography DLL
msports.dll	10.0.19041.1	Ports Class Installer
msrating.dll	10.0.19041.1	"msrating.DYNLINK"
msrawimage.dll	10.0.19041.1	MS RAW Image Decoder DLL
msrd2x40.dll	4.0.9801.18	Microsoft (R) Red ISAM
msrd3x40.dll	4.0.9801.25	Microsoft (R) Red ISAM
msrdc.dll	10.0.19041.1	Remote Differential Compression COM server
msrdpwebaccess.dll	10.0.19041.1	Microsoft Remote Desktop Services Web Access Control
msrepl40.dll	4.0.9801.0	Microsoft Replication Library
msrle32.dll	10.0.19041.1	Microsoft RLE Compressor
mssccntrs.dll	7.0.19041.488	PKM Perfmon Counter DLL
mssign32.dll	10.0.19041.1	Microsoft Trust Signing APIs
mssip32.dll	10.0.19041.1	MSSIP32 Forwarder DLL
mssitlb.dll	7.0.19041.488	mssitlb
msspellcheckingfacility.dll	10.0.19041.329	Microsoft Spell Checking Facility
mssph.dll	7.0.19041.488	Microsoft Search Protocol Handler
mssprxy.dll	7.0.19041.488	Microsoft Search Proxy

Navigation

mssrch.dll	7.0.19041.488	Microsoft Embedded Search
msstkprp.dll	6.1.98.16	msprop32.ocx
mssvp.dll	7.0.19041.488	MSSearch Vista Platform
mstask.dll	10.0.19041.1	Task Scheduler interface DLL
mstext40.dll	4.0.9801.26	Microsoft Jet Text Isam
mstscax.dll	10.0.19041.423	Remote Desktop Services ActiveX Client
msutb.dll	10.0.19041.1	MSUTB Server DLL
msv1_0.dll	10.0.19041.450	Microsoft Authentication Package v1.0
msvbvm60.dll	6.0.98.15	Visual Basic Virtual Machine
msvcirt.dll	7.0.19041.1	Windows NT IOStreams DLL
msvcp_win.dll	10.0.19041.488	Microsoft® C Runtime Library
msvcp100.dll	10.0.40219.325	Microsoft® C Runtime Library
msvcp110.dll	11.0.51106.1	Microsoft® C Runtime Library
msvcp110_win.dll	10.0.19041.1	Microsoft® STL110 C++ Runtime Library
msvcp120.dll	12.0.40660.0	Microsoft® C Runtime Library
msvcp120_clr0400.dll	12.0.52519.0	Microsoft® C Runtime Library
msvcp140.dll	14.24.28127.4	Microsoft® C Runtime Library
msvcp140_1.dll	14.24.28127.4	Microsoft® C Runtime Library _1
msvcp140_2.dll	14.24.28127.4	Microsoft® C Runtime Library _2
msvcp140_clr0400.dll	14.10.25028.0	Microsoft® C Runtime Library
msvcp140_codecvt_ids.dll	14.24.28127.4	Microsoft® C Runtime Library _codecvt_ids
msvcp60.dll	7.0.19041.1	Windows NT C++ Runtime Library DLL
msvcr100.dll	10.0.40219.325	Microsoft® C Runtime Library
msvcr100_clr0400.dll	14.8.4084.0	Microsoft® .NET Framework
msvcr110.dll	11.0.51106.1	Microsoft® C Runtime Library
msvcr120.dll	12.0.40660.0	Microsoft® C Runtime Library
msvcr120_clr0400.dll	12.0.52519.0	Microsoft® C Runtime Library
msvcrt.dll	7.0.19041.1	Windows NT CRT DLL
msvcrt20.dll	2.12.0.0	Microsoft® C Runtime Library
msvcrt40.dll	10.0.19041.1	VC 4.x CRT DLL (Forwarded to msvcrt.dll)
msvfw32.dll	10.0.19041.1	Microsoft Video for Windows DLL
msvidc32.dll	10.0.19041.1	Microsoft Video 1 Compressor
msvidctl.dll	6.5.19041.329	ActiveX control for streaming video
msvideodsp.dll	10.0.19041.1	Video Stabilization MFT
msvp9dec.dll	10.0.19041.1	Windows VP9 Video Decoder
msvproc.dll	10.0.19041.488	Media Foundation Video Processor
msvpxenc.dll	10.0.19041.1	Windows VPX Video Encoder
mswb7.dll	10.0.19041.1	MSWB7 DLL
mswdat10.dll	4.0.9801.0	Microsoft Jet Sort Tables
mswebp.dll	10.0.19041.1	WEBP DLL
mswmdm.dll	12.0.19041.329	Windows Media Device Manager Core
mswsock.dll	10.0.19041.423	Microsoft Windows Sockets 2.0 Service Provider
mswstr10.dll	4.0.9801.1	Microsoft Jet Sort Library
msxactps.dll	10.0.19041.1	OLE DB Transaction Proxies/Stubs
msxactps.dll	10.0.19041.1	OLE DB Transaction Proxies/Stubs
msxbde40.dll	4.0.9801.25	Microsoft Jet xBASE Isam
msxml3.dll	8.110.19041.1	MSXML 3.0
msxml3r.dll	8.110.19041.1	XML Resources
msxml6.dll	6.30.19041.388	MSXML 6.0
msxml6r.dll	6.30.19041.388	XML Resources
msyuv.dll	10.0.19041.1	Microsoft UYVY Video Decompressor
mtf.dll	10.0.19041.1	"MTF.DYNLINK"
mtxclu.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator Failover Clustering Support DLL
mtxdm.dll	2001.12.10941.16384	COM+
mtxex.dll	2001.12.10941.16384	COM+

mtxlegih.dll	2001.12.10941.16384	COM+
mtxoci.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator Dat
muifontsetup.dll	10.0.19041.1	MUI Callback for font registry settings
mycomput.dll	10.0.19041.1	Computer Management
mydocs.dll	10.0.19041.1	My Documents Folder UI
napcrypt.dll	10.0.19041.1	NAP Cryptographic API helper
napinsp.dll	10.0.19041.1	E-mail Naming Shim Provider
naturallanguage6.dll	10.0.19041.1	Natural Language Development Platform 6
ncaapi.dll	10.0.19041.1	Microsoft Network Connectivity Assistant API
ncdprop.dll	10.0.19041.1	Advanced network device properties
nci.dll	10.0.19041.1	CoInstaller: NET
ncobjapi.dll	10.0.19041.1	Microsoft® Windows® Operating System
ncrypt.dll	10.0.19041.1	Windows NCrypt Router
ncryptprov.dll	10.0.19041.1	Microsoft KSP
ncryptsslp.dll	10.0.19041.1	Microsoft SChannel Provider
nddeapi.dll	10.0.19041.1	Network DDE Share Management APIs
ndfapi.dll	10.0.19041.1	Network Diagnostic Framework Client API
ndfetw.dll	10.0.19041.1	Network Diagnostic Engine Event Interface
ndfhcdiscovery.dll	10.0.19041.1	Network Diagnostic Framework HC Discovery API
ndishc.dll	10.0.19041.1	NDIS Helper Classes
ndproxystub.dll	10.0.19041.1	Network Diagnostic Engine Proxy/Stub
negoexts.dll	10.0.19041.1	NegoExtender Security Package
netapi32.dll	10.0.19041.1	Net Win32 API DLL
netbios.dll	10.0.19041.1	NetBIOS Interface Library
netcenter.dll	10.0.19041.423	Network Center control panel
netcfgx.dll	10.0.19041.1	Network Configuration Objects
netcorehc.dll	10.0.19041.1	Networking Core Diagnostics Helper Classes
netdiagfx.dll	10.0.19041.1	Network Diagnostic Framework
netdriverinstall.dll	10.0.19041.1	Network Driver Installation
netevent.dll	10.0.19041.1	Net Event Handler
netfxperf.dll	10.0.19041.1	Extensible Performance Counter Shim
neth.dll	10.0.19041.1	Net Help Messages DLL
netid.dll	10.0.19041.1	System Control Panel Applet; Network ID Page
netiohlp.dll	10.0.19041.1	Netio Helper DLL
netjoin.dll	10.0.19041.1	Domain Join DLL
netlogon.dll	10.0.19041.450	Net Logon Services DLL
netmsg.dll	10.0.19041.1	Net Messages DLL
netplwiz.dll	10.0.19041.1	Map Network Drives/Network Places Wizard
netprofm.dll	10.0.19041.329	Network List Manager
netprovfw.dll	10.0.19041.1	Provisioning Service Framework DLL
netprovisionsp.dll	10.0.19041.1	Provisioning Service Provider DLL
netsetupapi.dll	10.0.19041.1	Network Configuration API
netsetupengine.dll	10.0.19041.1	Network Configuration Engine
netsetupshim.dll	10.0.19041.1	Network Configuration API
netshell.dll	10.0.19041.329	Network Connections Shell
netutils.dll	10.0.19041.1	Net Win32 API Helpers DLL
networkcollectionagent.dll	11.0.19041.1	Network Collection Agent
networkexplorer.dll	10.0.19041.1	Network Explorer
networkhelper.dll	10.0.19041.1	Network utilities for mail, contacts, calendar
networkitemfactory.dll	10.0.19041.1	NetworkItem Factory
newdev.dll	6.0.5054.0	Add Hardware Device Library
ngccredprov.dll	10.0.19041.1	Microsoft Passport Credential Provider
ngckeyenum.dll	10.0.19041.1	Microsoft Passport Key Enumeration Manager
ngcksp.dll	10.0.19041.1	Microsoft Passport Key Storage Provider
ngclocal.dll	10.0.19041.1	NGC Local Account APIs

ninput.dll	10.0.19041.1	Microsoft Pen and Touch Input Component
nlaapi.dll	10.0.19041.1	Network Location Awareness 2
nlhtml.dll	2008.0.19041.1	HTML filter
nlmgp.dll	10.0.19041.1	Network List Manager Snapin
nlmproxy.dll	10.0.19041.117	Network List Manager Public Proxy
nlmsprep.dll	10.0.19041.117	Network List Manager Sysprep Module
nlsbres.dll	10.0.19041.1	NLSBuild resource DLL
nlsdata0000.dll	10.0.19041.1	Microsoft Neutral Natural Language Server Data and Code
nlsdata0009.dll	10.0.19041.1	Microsoft English Natural Language Server Data and Code
nlsdata002a.dll	10.0.19041.1	Microsoft Neutral Natural Language Server Data and Code
nlsdl.dll	10.0.19041.1	Nls Downlevel DLL
nmadirect.dll	10.0.19041.1	Nma Direct
normaliz.dll	10.0.19041.1	Unicode Normalization DLL
npmproxy.dll	10.0.19041.117	Network List Manager Proxy
npsm.dll	10.0.19041.329	NPSM
npsmdesktopprovider.dll	10.0.19041.1	<d> NPSM Desktop Local Provider DLL
nshhttp.dll	10.0.19041.1	HTTP netsh DLL
nshipsec.dll	10.0.19041.1	Net Shell IP Security helper DLL
nshwfp.dll	10.0.19041.488	Windows Filtering Platform Netsh Helper
nsi.dll	10.0.19041.1	NSI User-mode interface DLL
ntasn1.dll	10.0.19041.1	Microsoft ASN.1 API
ntdll.dll	10.0.19041.488	NT Layer DLL
ntdsapi.dll	10.0.19041.1	Active Directory Domain Services API
ntlanman.dll	10.0.19041.488	Microsoft® Lan Manager
ntlanui2.dll	10.0.19041.1	Network object shell UI
ntlmshared.dll	10.0.19041.1	NTLM Shared Functionality
ntmarta.dll	10.0.19041.1	Windows NT MARTA provider
ntprint.dll	10.0.19041.1	Spooler Setup DLL
ntshrui.dll	10.0.19041.488	Shell extensions for sharing
ntvdm64.dll	10.0.19041.423	16-bit Emulation on NT64
objsel.dll	10.0.19041.1	Object Picker Dialog
occache.dll	11.0.19041.1	Object Control Viewer
ocsetapi.dll	10.0.19041.1	Windows Optional Component Setup API
odbc32.dll	10.0.19041.1	ODBC Driver Manager
odbcbcp.dll	10.0.19041.1	BCP for ODBC
odbcconf.dll	10.0.19041.388	ODBC Driver Configuration Program
odbccp32.dll	10.0.19041.1	ODBC Installer
odbccr32.dll	10.0.19041.1	ODBC Cursor Library
odbccu32.dll	10.0.19041.1	ODBC Cursor Library
odbcint.dll	10.0.19041.1	ODBC Resources
odbcji32.dll	10.0.19041.1	Microsoft ODBC Desktop Driver Pack 3.5
odbcjt32.dll	10.0.19041.1	Microsoft ODBC Desktop Driver Pack 3.5
odbctrac.dll	10.0.19041.1	ODBC Driver Manager Trace
oddbse32.dll	10.0.19041.1	ODBC (3.0) driver for DBase
odexl32.dll	10.0.19041.1	ODBC (3.0) driver for Excel
odfox32.dll	10.0.19041.1	ODBC (3.0) driver for FoxPro
odpdx32.dll	10.0.19041.1	ODBC (3.0) driver for Paradox
odtext32.dll	10.0.19041.1	ODBC (3.0) driver for text files
oemlicense.dll	10.0.19041.508	Client Licensing Platform Client Provisioning
offfilt.dll	2008.0.19041.1	OFFICE Filter
offlinelsa.dll	10.0.19041.1	Windows
offlinesam.dll	10.0.19041.1	Windows
offreg.dll	10.0.19041.1	Offline registry DLL
ole2.dll	3.10.0.103	Windows Win16 Application Launcher
ole2disp.dll	3.10.0.103	Windows Win16 Application Launcher

Navigation

Navigation

ole2nls.dll	3.10.0.103	Windows Win16 Application Launcher
ole32.dll	10.0.19041.84	Microsoft OLE for Windows
oleacc.dll	7.2.19041.1	Active Accessibility Core Component
oleacchooks.dll	7.2.19041.1	Active Accessibility Event Hooks Library
oleaccrc.dll	7.2.19041.1	Active Accessibility Resource DLL
oleaut32.dll	10.0.19041.388	OLEAUT32.DLL
olecli32.dll	10.0.19041.1	Object Linking and Embedding Client Library
oledb32.dll	10.0.19041.329	OLE DB Core Services
oledb32.dll	10.0.19041.329	OLE DB Core Services
oledb32r.dll	10.0.19041.1	OLE DB Core Services Resources
oledb32r.dll	10.0.19041.1	OLE DB Core Services Resources
oledlg.dll	10.0.19041.1	OLE User Interface Support
oleprn.dll	10.0.19041.329	Oleprn DLL
olepro32.dll	10.0.19041.84	OLEPRO32.DLL
olesvr32.dll	10.0.19041.1	Object Linking and Embedding Server Library
olethk32.dll	10.0.19041.1	Microsoft OLE for Windows
omadmapi.dll	10.0.19041.488	omadmapi
ondemandbrokerclient.dll	10.0.19041.1	OnDemandBrokerClient
ondemandconnroutehelper.dll	10.0.19041.1	On Demand Connctiond Route Helper
onecorecommonproxystub.dll	10.0.19041.1	OneCore Common Proxy Stub
onecoreuapcommonproxystub.dll	10.0.19041.508	OneCoreUAP Common Proxy Stub
onedrivesettingsyncprovider.dll	10.0.19041.1	OneDrive Setting Sync
onex.dll	10.0.19041.1	IEEE 802.1X supplicant library
onexui.dll	10.0.19041.1	IEEE 802.1X supplicant UI library
onnxruntime.dll	1.0.1911.2111	ONNX Runtime
opcservices.dll	10.0.19041.1	Native Code OPC Services Library
opencl.dll	1.2.11.0	OpenCL Client DLL
opengl32.dll	10.0.19041.488	OpenGL Client DLL
ortcengine.dll	2018.6.1.57	Microsoft Skype ORTC Engine
osbaseln.dll	10.0.19041.1	Service Reporting API
osuninst.dll	10.0.19041.1	Uninstall Interface
p2p.dll	10.0.19041.1	Peer-to-Peer Grouping
p2pgraph.dll	10.0.19041.1	Peer-to-Peer Graphing
p2pnetsh.dll	10.0.19041.1	Peer-to-Peer NetSh Helper
packager.dll	10.0.19041.1	Object Packager2
packagestateroaming.dll	10.0.19041.1	Package State Roaming
panmap.dll	10.0.19041.1	PANOSE(tm) Font Mapper
pautoenr.dll	10.0.19041.1	Auto Enrollment DLL
payloadrestrictions.dll	10.0.19041.1	Payload Restrictions Mitigation Provider
paymentmediatorserviceproxy.dll	10.0.19041.1	Payment Mediator Service Proxy
pcacli.dll	10.0.19041.423	Program Compatibility Assistant Client Module
pcaui.dll	10.0.19041.423	Program Compatibility Assistant User Interface Module
pcpksp.dll	10.0.19041.488	Microsoft Platform Key Storage Provider for Platform Crypto Provider
pcshellcommonproxystub.dll	10.0.19041.488	PCShell Common Proxy Stub
pcwum.dll	10.0.19041.1	Performance Counters for Windows Native DLL
pdh.dll	10.0.19041.488	Windows Performance Data Helper DLL
pdhui.dll	10.0.19041.1	PDH UI
peerdist.dll	10.0.19041.1	BranchCache Client Library
peerdistsh.dll	10.0.19041.1	BranchCache Netshell Helper
peopleapis.dll	10.0.19041.264	DLL for PeopleRT
perceptiondevice.dll	10.0.19041.1	Perception Device
perceptionsimulation.proxystubs.dll	10.0.19041.1	Windows Perception Simulation Proxy Stubs
perfctrs.dll	10.0.19041.488	Performance Counters
perfdisk.dll	10.0.19041.488	Windows Disk Performance Objects DLL
perfnet.dll	10.0.19041.488	Windows Network Service Performance Objects DLL

perfos.dll	10.0.19041.488	Windows System Performance Objects DLL
perfproc.dll	10.0.19041.488	Windows System Process Performance Objects Dl
perfts.dll	10.0.19041.1	Windows Remote Desktop Services Performance Objects
phonecallhistoryapis.dll	10.0.19041.264	DLL for PhoneCallHistoryRT
phoneom.dll	10.0.19041.264	Phone Object Model
phoneplatformabstraction.dll	10.0.19041.1	Phone Platform Abstraction
phoneutil.dll	10.0.19041.1	Phone utilities
phoneutilres.dll	10.0.19041.1	Resource DLL for Phone utilities
photometadatahandler.dll	10.0.19041.1	Photo Metadata Handler
photowiz.dll	10.0.19041.1	Photo Printing Wizard
pickerplatform.dll	10.0.19041.388	PickerPlatform
pid.dll	10.0.19041.1	Microsoft PID
pidgenx.dll	10.0.19041.1	Pid Generation
pifmgr.dll	10.0.19041.1	Windows NT PIF Manager Icon Resources Library
pimindexmaintenanceclient.dll	10.0.19041.1	Client dll for Pim Index Maintenance
pimstore.dll	10.0.19041.1	POOM
pku2u.dll	10.0.19041.388	Pku2u Security Package
pla.dll	10.0.19041.1	Performance Logs & Alerts
playlistfolder.dll	10.0.19041.1	Playlist Folder
playsndsrv.dll	10.0.19041.1	PlaySound Service
playtodevice.dll	10.0.19041.1	PLAYTODEVICE DLL
playtomanager.dll	10.0.19041.388	Microsoft Windows PlayTo Manager
playtomenu.dll	12.0.19041.1	Cast to Device Menu DLL
playtoreceiver.dll	10.0.19041.1	DLNA DMR DLL
playtostatusprovider.dll	10.0.19041.1	PlayTo Status Provider Dll
pngfilt.dll	11.0.19041.1	IE PNG plugin image decoder
pnrpnsp.dll	10.0.19041.1	PNRP Name Space Provider
policymanager.dll	10.0.19041.508	Policy Manager DLL
polstore.dll	10.0.19041.1	Policy Storage dll
portabledeviceapi.dll	10.0.19041.1	Windows Portable Device API Components
portabledeviceclassextension.dll	10.0.19041.1	Windows Portable Device Class Extension Component
portabledeviceconnectapi.dll	10.0.19041.1	Portable Device Connection API Components
portabledevicestatus.dll	10.0.19041.1	Microsoft Windows Portable Device Status Provider
portabledevicesyncprovider.dll	10.0.19041.1	Microsoft Windows Portable Device Provider.
portabledevicetypes.dll	10.0.19041.1	Windows Portable Device (Parameter) Types Component
portabledevicewiacompat.dll	10.0.19041.1	PortableDevice WIA Compatibility Driver
posyncservices.dll	10.0.19041.1	Change Tracking
pots.dll	10.0.19041.1	Power Troubleshooter
powercpl.dll	10.0.19041.423	Power Options Control Panel
powrprof.dll	10.0.19041.1	Power Profile Helper DLL
presentationcffrasterizernative_v0300.dll	3.0.6920.9141	WinFX OpenType/CFF Rasterizer
presentationhostproxy.dll	10.0.19041.1	Windows Presentation Foundation Host Proxy
presentationnative_v0300.dll	3.0.6920.9141	PresentationNative_v0300.dll
prflbmsg.dll	10.0.19041.1	Perflib Event Messages
print.workflow.source.dll	10.0.19041.388	Microsoft Windows Print Workflow Source App Library
printconfig.dll	0.3.19041.508	PrintConfig User Interface
printplatformconfig.dll	10.0.19041.1	Legacy Print Platform Adapter
printui.dll	10.0.19041.1	Printer Settings User Interface
printworkflowproxy.dll	10.0.19041.388	Microsoft Windows Print Workflow Proxy
printworkflowservice.dll	10.0.19041.388	Microsoft Windows Print Workflow Service Internal
printwsdahost.dll	10.0.19041.388	PrintWSDAHost
prncache.dll	10.0.19041.1	Print UI Cache
prnfldr.dll	10.0.19041.1	prnfldr dll
prnntfy.dll	10.0.19041.488	prnntfy DLL
prntvpt.dll	10.0.19041.1	Print Ticket Services Module

Navigation

Navigation

profapi.dll	10.0.19041.488	User Profile Basic API
profext.dll	10.0.19041.153	profext
propsys.dll	7.0.19041.488	Microsoft Property System
provcore.dll	10.0.19041.1	Microsoft Wireless Provisioning Core
provisioningcommandscsp.dll	10.0.19041.1	Provisioning package command configuration service provider
provmigrate.dll	10.0.19041.1	Provisioning Migration Handler
provplatformdesktop.dll	10.0.19041.1	Provisioning platform for desktop editions
provsvc.dll	10.0.19041.1	Windows HomeGroup
provthrd.dll	10.0.19041.1	WMI Provider Thread & Log Library
proximitycommon.dll	10.0.19041.1	Proximity Common Implementation
proximitycommonpal.dll	10.0.19041.1	Proximity Common PAL
proximityrtapipal.dll	10.0.19041.1	Proximity WinRT API PAL
prvdmofcomp.dll	10.0.19041.1	WMI
psapi.dll	10.0.19041.1	Process Status Helper
pshed.dll	10.0.19041.1	Platform Specific Hardware Error Driver
psisdecd.dll	10.0.19041.329	Microsoft SI/PSI parser for MPEG2 based networks.
psmodulediscoveryprovider.dll	10.0.19041.1	WMI
pstorec.dll	10.0.19041.1	Deprecated Protected Storage COM interfaces
puiapi.dll	10.0.19041.423	puiapi DLL
puiobj.dll	10.0.19041.423	PrintUI Objects DLL
pwrshplugin.dll	10.0.19041.1	pwrshplugin.dll
qasf.dll	12.0.19041.1	DirectShow ASF Support
qcap.dll	10.0.19041.1	DirectShow Runtime.
qdv.dll	10.0.19041.1	DirectShow Runtime.
qdvd.dll	10.0.19041.329	DirectShow DVD PlayBack Runtime.
qedit.dll	10.0.19041.329	DirectShow Editing.
qedwipes.dll	10.0.19041.1	DirectShow Editing SMPTE Wipes
quartz.dll	10.0.19041.329	DirectShow Runtime.
query.dll	10.0.19041.1	Content Index Utility DLL
qwave.dll	10.0.19041.1	Windows NT
racengn.dll	10.0.19041.1	Reliability analysis metrics calculation engine
racpldlg.dll	10.0.19041.1	Remote Assistance Contact List
radardt.dll	10.0.19041.1	Microsoft Windows Resource Exhaustion Detector
radarrs.dll	10.0.19041.1	Microsoft Windows Resource Exhaustion Resolver
radcui.dll	10.0.19041.423	RemoteApp and Desktop Connection UI Component
rasadhlp.dll	10.0.19041.1	Remote Access AutoDial Helper
rasapi32.dll	10.0.19041.450	Remote Access API
raschap.dll	10.0.19041.1	Remote Access PPP CHAP
raschapext.dll	10.0.19041.1	Windows Extension library for raschap
rasctrs.dll	10.0.19041.1	Windows NT Remote Access Perfmon Counter dll
rasdiag.dll	10.0.19041.1	RAS Diagnostics Helper Classes
rasdlg.dll	10.0.19041.450	Remote Access Common Dialog API
rasgcw.dll	10.0.19041.450	RAS Wizard Pages
rasman.dll	10.0.19041.1	Remote Access Connection Manager
rasmontr.dll	10.0.19041.1	RAS Monitor DLL
rasplap.dll	10.0.19041.450	RAS PLAP Credential Provider
rasppp.dll	10.0.19041.1	Remote Access PPP
rastapi.dll	10.0.19041.1	Remote Access TAPI Compliance Layer
rastls.dll	10.0.19041.1	Remote Access PPP EAP-TLS
rastlsext.dll	10.0.19041.1	Windows Extension library for rastls
rdpbase.dll	10.0.19041.84	Rdp OneCore Base Services
rdpcore.dll	10.0.19041.84	RDP Core DLL
rdpencom.dll	10.0.19041.329	RDPSRAPI COM Objects
rdpendp.dll	10.0.19041.1	RDP Audio Endpoint
rdpsaps.dll	10.0.19041.1	RDP Session Agent Proxy Stub

Navigation

rdpserverbase.dll	10.0.19041.84	Rdp Server OneCore Base Services
rdpsharercom.dll	10.0.19041.329	RDPSRAPI Sharer COM Objects
rdpviewerax.dll	10.0.19041.329	RDPSRAPI Viewer COM Objects and ActiveX
rdvgocl32.dll	10.0.19041.488	Microsoft RemoteFX OpenCL ICD
rdvgogl32.dll	10.0.19041.488	Microsoft RemoteFX OpenGL
rdvgu1132.dll	10.0.19041.488	Microsoft RemoteFX Virtual GPU
rdvgumd32.dll	10.0.19041.488	Microsoft RemoteFX Virtual GPU
rdvvmtransport.dll	10.0.19041.1	RdvVmTransport EndPoints
reagent.dll	10.0.19041.84	Microsoft Windows Recovery Agent DLL
regapi.dll	10.0.19041.1	Registry Configuration APIs
regctrl.dll	10.0.19041.1	RegCtrl
reguwpapi.dll	10.0.19041.1	UWP Registry API
reinfo.dll	10.0.19041.1	Microsoft Windows Recovery Info DLL
remoteaudioendpoint.dll	10.0.19041.1	Remote Audio Endpoint
remotepg.dll	10.0.19041.1	Remote Sessions CPL Extension
removedevicecontexthandler.dll	10.0.19041.1	Devices & Printers Remove Device Context Menu Handler
removedeviceelevated.dll	10.0.19041.1	RemoveDeviceElevated Proxy Dll
resampledmo.dll	10.0.19041.1	Windows Media Resampler
resourcepolicyclient.dll	10.0.19041.388	Resource Policy Client
resutils.dll	10.0.19041.488	Microsoft Cluster Resource Utility DLL
rfxvmt.dll	10.0.19041.1	Microsoft RemoteFX VM Transport
rgb9rast.dll	10.0.19041.1	Microsoft® Windows® Operating System
riched20.dll	5.31.23.1231	Rich Text Edit Control, v3.1
riched32.dll	10.0.19041.1	Wrapper Dll for Richedit 1.0
rltkapo.dll	11.0.6000.704	Realtek(r) LFX/GFX DSP component
rmclient.dll	10.0.19041.1	Resource Manager Client
rnr20.dll	10.0.19041.1	Windows Socket2 NameSpace DLL
rometadata.dll	4.8.3673.0	Microsoft MetaData Library
rpchttp.dll	10.0.19041.1	RPC HTTP DLL
rpcns4.dll	10.0.19041.1	Remote Procedure Call Name Service Client
rpcnsh.dll	10.0.19041.1	RPC Netshell Helper
rpcrt4.dll	10.0.19041.508	Remote Procedure Call Runtime
rpcrtremote.dll	10.0.19041.1	Remote RPC Extension
rsaenh.dll	10.0.19041.1	Microsoft Enhanced Cryptographic Provider
rshx32.dll	10.0.19041.1	Security Shell Extension
rstrtmgr.dll	10.0.19041.1	Restart Manager
rtffilt.dll	2008.0.19041.1	RTF Filter
rtm.dll	10.0.19041.450	Routing Table Manager
rtmcodecs.dll	2018.6.1.57	Microsoft Real Time Media Codec Library
rtmediaframe.dll	10.0.19041.388	Windows Runtime MediaFrame DLL
rtmmvrortc.dll	2018.6.1.57	Microsoft Real Time Media ORTC Video Renderer
rtmpal.dll	2018.6.1.57	Microsoft Real Time Media Stack PAL
rtmpltfm.dll	2018.6.1.57	Microsoft Real Time Media Stack
rtutils.dll	10.0.19041.508	Routing Utilities
rtworkq.dll	10.0.19041.1	Realtime WorkQueue DLL
samcli.dll	10.0.19041.1	Security Accounts Manager Client DLL
samlib.dll	10.0.19041.1	SAM Library DLL
sas.dll	10.0.19041.1	WinLogon Software SAS Library
sbe.dll	10.0.19041.1	DirectShow Stream Buffer Filter.
sbeio.dll	12.0.19041.1	Stream Buffer IO DLL
sberes.dll	10.0.19041.1	DirectShow Stream Buffer Filter Resouces.
scansetting.dll	10.0.19041.1	Microsoft® Windows(TM) ScanSettings Profile and Scanning implementation
scarddlg.dll	10.0.19041.1	SCardDlg - Smart Card Common Dialog
scecli.dll	10.0.19041.450	Windows Security Configuration Editor Client Engine
scesrv.dll	10.0.19041.488	Windows Security Configuration Editor Engine

Navigation

schannel.dll	10.0.19041.508	TLS / SSL Security Provider
schedcli.dll	10.0.19041.1	Scheduler Service Client DLL
scksp.dll	10.0.19041.1	Microsoft Smart Card Key Storage Provider
scripto.dll	6.6.19041.1	Microsoft ScriptO
scrobj.dll	5.812.10240.16384	Windows ® Script Component Runtime
scrptadm.dll	10.0.19041.1	Script Adm Extension
scrrun.dll	5.812.10240.16384	Microsoft ® Script Runtime
sdiageng.dll	10.0.19041.1	Scripted Diagnostics Execution Engine
sdiagprv.dll	10.0.19041.1	Windows Scripted Diagnostic Provider API
sdohlp.dll	10.0.19041.1	NPS SDO Helper Component
search.protocolhandler.mapi2.dll	7.0.19041.488	Microsoft Search Protocol Handler for MAPI2
searchfolder.dll	10.0.19041.1	SearchFolder
sechost.dll	10.0.19041.388	Host for SCM/SDDL/LSA Lookup APIs
secomn32.dll	2.0.8.40	SECOMN.DLL
secproc.dll	10.0.19041.1	Windows Rights Management Desktop Security Processor
secproc_isv.dll	10.0.19041.1	Windows Rights Management Desktop Security Processor
secproc_ssp.dll	10.0.19041.1	Windows Rights Management Services Server Security Processor
secproc_ssp_isv.dll	10.0.19041.1	Windows Rights Management Services Server Security Processor (Pre-production)
secur32.dll	10.0.19041.1	Security Support Provider Interface
security.dll	10.0.19041.1	Security Support Provider Interface
securitycenterbrokerps.dll	10.0.19041.329	SecurityCenterBrokerPS
sehdhf32.dll	2.0.8.40	SEHDHF.DLL
semgrps.dll	10.0.19041.1	SEMgrSvc Proxy
sendmail.dll	10.0.19041.1	Send Mail
sensapi.dll	10.0.19041.1	SENS Connectivity API DLL
sensorsapi.dll	10.0.19041.329	Sensor API
sensorscpl.dll	10.0.19041.1	Open Location and Other Sensors
sensorsnativeapi.dll	10.0.19041.1	Sensors Native API
sensorsnativeapi.v2.dll	10.0.19041.1	Sensors Native API (V2 stack)
sensorsutilsv2.dll	10.0.19041.1	Sensors v2 Utilities DLL
serialui.dll	10.0.19041.1	Serial Port Property Pages
serwvdrv.dll	10.0.19041.1	Unimodem Serial Wave driver
sessenv.dll	10.0.19041.1	Remote Desktop Configuration service
settingmonitor.dll	10.0.19041.1	Setting Synchronization Change Monitor
settingsync.dll	10.0.19041.1	Setting Synchronization
settingsynccore.dll	10.0.19041.388	Setting Synchronization Core
setupapi.dll	10.0.19041.1	Windows Setup API
setupcl.dll	10.0.19041.423	System Clone Library
setupcln.dll	10.0.19041.1	Setup Files Cleanup
sfc.dll	10.0.19041.1	Windows File Protection
sfc_os.dll	10.0.19041.1	Windows File Protection
sfcom.dll	3.0.0.11	SFCOM.DLL
shacct.dll	10.0.19041.1	Shell Accounts Classes
shacctprofile.dll	10.0.19041.1	Shell Accounts Profile Classes
sharehost.dll	10.0.19041.488	ShareHost
shcore.dll	10.0.19041.488	SHCORE
shdocvw.dll	10.0.19041.1	Shell Doc Object and Control Library
shell32.dll	10.0.19041.488	Windows Shell Common Dll
shellcommoncommonproxystub.dll	10.0.19041.488	ShellCommon Common Proxy Stub
shellstyle.dll	10.0.19041.1	Windows Shell Style Resource Dll
shfolder.dll	10.0.19041.1	Shell Folder Service
shgina.dll	10.0.19041.1	Windows Shell User Logon
shimeng.dll	10.0.19041.1	Shim Engine DLL
shimgvw.dll	10.0.19041.1	Photo Gallery Viewer
shlwapi.dll	10.0.19041.1	Shell Light-weight Utility Library

Navigation

shpafact.dll	10.0.19041.1	Windows Shell LUA/PA Elevation Factory Dll
shsetup.dll	10.0.19041.1	Shell setup helper
shsvcs.dll	10.0.19041.1	Windows Shell Services Dll
shunimpl.dll	10.0.19041.1	Windows Shell Obsolete APIs
shutdownext.dll	10.0.19041.1	Shutdown Graphic User Interface
shwebsvc.dll	10.0.19041.1	Windows Shell Web Services
signdrv.dll	10.0.19041.1	WMI provider for Signed Drivers
simauth.dll	10.0.19041.1	EAP SIM run-time dll
simcfg.dll	10.0.19041.1	EAP SIM config dll
slc.dll	10.0.19041.1	Software Licensing Client Dll
slcext.dll	10.0.19041.388	Software Licensing Client Extension Dll
slwga.dll	10.0.19041.1	Software Licensing WGA API
smartcardcredentialprovider.dll	10.0.19041.488	Windows Smartcard Credential Provider
smartscreenps.dll	10.0.19041.1	SmartScreenPS
smbhelperclass.dll	1.0.0.1	SMB (File Sharing) Helper Class for Network Diagnostic Framework
smphost.dll	10.0.19041.1	Storage Management Provider (SMP) host service
sndvolsso.dll	10.0.19041.1	SCA Volume
snmpapi.dll	10.0.19041.1	SNMP Utility Library
socialapis.dll	10.0.19041.264	DLL for SocialRT
softkbd.dll	10.0.19041.1	Soft Keyboard Server and Tip
softpub.dll	10.0.19041.1	Softpub Forwarder DLL
sortserver2003compat.dll	10.0.19041.1	Sort Version Server 2003
sortwindows61.dll	10.0.19041.1	SortWindows61 Dll
sortwindows62.dll	10.0.19041.1	SortWindows62 Dll
sortwindows6compat.dll	10.0.19041.1	Sort Version Windows 6.0
spacebridge.dll	10.0.19041.1	SpaceBridge
spatializerapo.dll	10.0.19041.423	Spatializer APO
spbcd.dll	10.0.19041.1	BCD Sysprep Plugin
spfileq.dll	10.0.19041.1	Windows SPFILEQ
spinf.dll	10.0.19041.1	Windows SPINF
spnet.dll	10.0.19041.1	Net Sysprep Plugin
spopk.dll	10.0.19041.1	OPK Sysprep Plugin
spp.dll	10.0.19041.1	Microsoft® Windows Shared Protection Point Library
sppc.dll	10.0.19041.1	Software Licensing Client Dll
sppcext.dll	10.0.19041.388	Software Protection Platform Client Extension Dll
sppcomapi.dll	10.0.19041.488	Software Licensing Library
sppinst.dll	10.0.19041.1	SPP CMI Installer Plug-in DLL
sppwmi.dll	10.0.19041.1	Software Protection Platform WMI provider
spwinsat.dll	10.0.19041.1	WinSAT Sysprep Plugin
spwizeng.dll	10.0.19041.329	Setup Wizard Framework
sqloledb.dll	10.0.19041.1	OLE DB Provider for SQL Server
sqloledb.dll	10.0.19041.1	OLE DB Provider for SQL Server
sqlsrv32.dll	10.0.19041.1	SQL Server ODBC Driver
sqlunirl.dll	2000.80.2039.0	String Function .DLL for SQL Enterprise Components
sqlwid.dll	2000.80.2039.0	Unicode Function .DLL for SQL Enterprise Components
sqlwoa.dll	2000.80.2040.0	Unicode/ANSI Function .DLL for SQL Enterprise Components
sqlxmlx.dll	10.0.19041.1	XML extensions for SQL Server
sqlxmlx.dll	10.0.19041.1	XML extensions for SQL Server
sqmapi.dll	10.0.19041.1	SQM Client
srchadmin.dll	7.0.19041.1	Indexing Options
srclient.dll	10.0.19041.1	Microsoft® Windows System Restore Client Library
srcom.dll	4.0.0.59	SRCOM.DLL
srm.dll	10.0.19041.1	Microsoft® File Server Resource Manager Common Library
srm_ps.dll	10.0.19041.1	Microsoft® FSRM internal proxy/stub
srmclient.dll	10.0.19041.450	Microsoft® File Server Resource Management Client Extensions

srmlib.dll	10.0.19041.1	Microsoft (R) File Server Resource Management I
srmscan.dll	10.0.19041.450	Microsoft® File Server Storage Reports Scan Eng
srmshell.dll	10.0.19041.1	Microsoft® File Server Resource Management Shell Extension
srmstormod.dll	10.0.19041.1	Microsoft® File Server Resource Management Office Parser
srmtrace.dll	10.0.19041.1	Microsoft® File Server Resource Management Tracing Library
srpapi.dll	10.0.19041.488	SRP APIs Dll
srpuxnativesnapin.dll	10.0.19041.1	Application Control Policies Group Policy Editor Extension
srumapi.dll	10.0.19041.207	System Resource Usage Monitor API
srumsvc.dll	10.0.19041.207	System Resource Usage Monitor Service
srvcli.dll	10.0.19041.1	Server Service Client DLL
sscore.dll	10.0.19041.1	Server Service Core DLL
ssdm.dll		
ssdpapi.dll	10.0.19041.1	SSDP Client API DLL
sspicli.dll	10.0.19041.488	Security Support Provider Interface
ssshim.dll	10.0.19041.1	Windows Componentization Platform Servicing API
startupscan.dll	10.0.19041.1	Startup scan task DLL
staterepository.core.dll	10.0.19041.508	StateRepository Core
stclient.dll	2001.12.10941.16384	COM+ Configuration Catalog Client
sti.dll	10.0.19041.264	Still Image Devices client DLL
stobject.dll	10.0.19041.1	Systray shell service object
storage.dll	3.10.0.103	Windows Win16 Application Launcher
storagecontexthandler.dll	10.0.19041.1	Device Center Storage Context Menu Handler
storagewmi.dll	10.0.19041.1	WMI Provider for Storage Management
storagewmi_passthru.dll	10.0.19041.1	WMI PassThru Provider for Storage Management
storprop.dll	10.0.19041.1	Property Pages for Storage Devices
structuredquery.dll	7.0.19041.388	Structured Query
sud.dll	10.0.19041.423	SUD Control Panel
sxproxy.dll	10.0.19041.1	Microsoft® Windows System Protection Proxy Library
sxs.dll	10.0.19041.450	Fusion 2.5
sxshared.dll	10.0.19041.1	Microsoft® Windows SX Shared Library
sxsstore.dll	10.0.19041.1	Sxs Store DLL
synccenter.dll	10.0.19041.423	Microsoft Sync Center
synccontroller.dll	10.0.19041.1	SyncController for managing sync of mail, contacts, calendar
synchostps.dll	10.0.19041.1	Proxystub for sync host
syncinfrastructure.dll	10.0.19041.1	Microsoft Windows Sync Infrastructure.
syncinfrastructureps.dll	10.0.19041.1	Microsoft Windows sync infrastructure proxy stub.
syncproxy.dll	10.0.19041.1	SyncProxy for RPC communication about sync of mail, contacts, calendar
syncreg.dll	2007.94.19041.1	Microsoft Synchronization Framework Registration
syncres.dll	10.0.19041.1	ActiveSync Resources
syncsettings.dll	10.0.19041.388	Sync Settings
syncutil.dll	10.0.19041.488	Sync utilities for mail, contacts, calendar
syssetup.dll	10.0.19041.1	Windows NT System Setup
systemcpl.dll	10.0.19041.423	My System CPL
systemeventsbrokerclient.dll	10.0.19041.1	system Events Broker Client Library
systemsettings.datamodel.dll	10.0.19041.388	SystemSettings.Datamodel private API
systemsupportinfo.dll	10.0.19041.1	Microsoft Windows operating system.
t2embed.dll	10.0.19041.264	Microsoft T2Embed Font Embedding
tapi3.dll	10.0.19041.329	Microsoft TAPI3
tapi32.dll	10.0.19041.423	Microsoft® Windows(TM) Telephony API Client DLL
tapimigplugin.dll	10.0.19041.1	Microsoft® Windows(TM) TAPI Migration Plugin Dll
tapiperf.dll	10.0.19041.1	Microsoft® Windows(TM) Telephony Performance Monitor
tapisrv.dll	10.0.19041.450	Microsoft® Windows(TM) Telephony Server
tapisysprep.dll	10.0.19041.1	Microsoft® Windows(TM) Telephony Sysprep Work
tapiui.dll	10.0.19041.1	Microsoft® Windows(TM) Telephony API UI DLL
taskapis.dll	10.0.19041.264	DLL for TaskRT

taskcomp.dll	10.0.19041.423	Task Scheduler Backward Compatibility Plug-in
taskschd.dll	10.0.19041.423	Task Scheduler COM API
taskschdps.dll	10.0.19041.1	Task Scheduler Interfaces Proxy
tbauth.dll	10.0.19041.1	TBAuth protocol handler
tbs.dll	10.0.19041.1	TBS
tcpipcfg.dll	10.0.19041.1	Network Configuration Objects
tcpmib.dll	10.0.19041.1	Standard TCP/IP Port Monitor Helper DLL
tcpmonui.dll	10.0.19041.1	Standard TCP/IP Port Monitor UI DLL
tdh.dll	10.0.19041.329	Event Trace Helper Library
tempsignedlicenseexchangetask.dll	10.0.19041.1	TempSignedLicenseExchangeTask Task
termmgr.dll	10.0.19041.329	Microsoft TAPI3 Terminal Manager
tetheringclient.dll	10.0.19041.1	Tethering Client
textinputframework.dll	10.0.19041.508	"TextInputFramework.DYNLINK"
textinputmethodformatter.dll		
textshaping.dll		
themecpl.dll	10.0.19041.423	Personalization CPL
themeui.dll	10.0.19041.1	Windows Theme API
threadpoolwinrt.dll	10.0.19041.1	Windows WinRT Threadpool
thumbcache.dll	10.0.19041.423	Microsoft Thumbnail Cache
tiledatarepository.dll	10.0.19041.450	Tile Data Repository
timedatemuicallback.dll	10.0.19041.1	Time Date Control UI Language Change plugin
tlscsp.dll	10.0.19041.1	Microsoft® Remote Desktop Services Cryptographic Utility
tokenbinding.dll	10.0.19041.1	Token Binding Protocol
tokenbroker.dll	10.0.19041.388	Token Broker
tokenbrokerui.dll	10.0.19041.1	Token Broker UI
tpmcertresources.dll	10.0.19041.1	TpmCertResources
tpmcompc.dll	10.0.19041.1	Computer Chooser Dialog
tpmcoreprovisioning.dll	10.0.19041.1	TPM Core Provisioning Library
tquery.dll	7.0.19041.488	Microsoft Tripoli Query
traffic.dll	10.0.19041.1	Microsoft Traffic Control 1.0 DLL
trustedsignalcredprov.dll	10.0.19041.1	TrustedSignal Credential Provider
tsbyuv.dll	10.0.19041.1	Toshiba Video Codec
tsgqec.dll	10.0.19041.388	RD Gateway QEC
tsmf.dll	10.0.19041.388	RDP MF Plugin
tspkg.dll	10.0.19041.264	Web Service Security Package
tsworkspace.dll	10.0.19041.1	RemoteApp and Desktop Connection Component
ttdloader.dll	10.0.19041.1	Time Travel Debugging Runtime Loader
ttdplm.dll	10.0.19041.1	Time Travel Debugger PLM APIs
ttdrecord.dll	10.0.19041.1	Time Travel Debugging Recording Manager
ttdrecordcpu.dll	10.0.19041.1	Time Travel Debugging CPU Recorder Runtime
ttlsauth.dll	10.0.19041.1	EAP TTLS run-time dll
ttlscfg.dll	10.0.19041.1	EAP TTLS configuration dll
ttlsext.dll	10.0.19041.1	Windows Extension library for EAP TTLS
tvratings.dll	10.0.19041.1	Module for managing TV ratings
twext.dll	10.0.19041.1	Previous Versions property page
twinapi.appcore.dll	10.0.19041.488	twinapi.appcore
twinapi.dll	10.0.19041.488	twinapi
twinui.appcore.dll	10.0.19041.488	TWINUI.APPCORE
twinui.dll	10.0.19041.488	TWINUI
txflog.dll	2001.12.10941.16384	COM+
txfw32.dll	10.0.19041.1	TxF Win32 DLL
typelib.dll	3.10.0.103	Windows Win16 Application Launcher
tzautoupdate.dll	10.0.19041.1	Auto Time Zone Updater
tzres.dll	10.0.19041.488	Time Zones resource DLL
ucmhc.dll	10.0.19041.1	UCM Helper Class

Navigation

Navigation

ucrtbase.dll	10.0.19041.488	Microsoft® C Runtime Library
ucrtbase_clr0400.dll	14.10.25028.0	Microsoft® C Runtime Library
udhisapi.dll	10.0.19041.508	UPnP Device Host ISAPI Extension
uexfat.dll	10.0.19041.1	eXfat Utility DLL
ufat.dll	10.0.19041.1	FAT Utility DLL
uiamanager.dll	10.0.19041.488	UiaManager
uianimation.dll	10.0.19041.1	Windows Animation Manager
uiautomationcore.dll	7.2.19041.488	Microsoft UI Automation Core
uicom.dll	10.0.19041.1	Add/Remove Modems
uimanagerbrokerps.dll	10.0.19041.1	Microsoft UIManager Broker Proxy Stub
uireng.dll	10.0.19041.1	UI Recording Engine Library
uiribbon.dll	10.0.19041.1	Windows Ribbon Framework
ulib.dll	10.0.19041.1	File Utilities Support DLL
umdmxfrm.dll	10.0.19041.1	Unimodem Tranform Module
umpdc.dll		
unenrollhook.dll	10.0.19041.423	unenrollhook DLL
unimdmat.dll	10.0.19041.1	Unimodem Service Provider AT Mini Driver
uniplat.dll	10.0.19041.1	Unimodem AT Mini Driver Platform Driver for Windows NT
unistore.dll	10.0.19041.1	Unified Store
untfs.dll	10.0.19041.1	NTFS Utility DLL
updatepolicy.dll	10.0.19041.508	Update Policy Reader
upnp.dll	10.0.19041.1	UPnP Control Point API
upnphost.dll	10.0.19041.508	UPnP Device Host
urefs.dll	10.0.19041.1	NTFS Utility DLL
urefsv1.dll	10.0.19041.1	NTFS Utility DLL
ureg.dll	10.0.19041.1	Registry Utility DLL
url.dll	11.0.19041.1	Internet Shortcut Shell Extension DLL
urlmon.dll	11.0.19041.488	OLE32 Extensions for Win32
usbceip.dll	10.0.19041.1	USBCEIP Task
usbperf.dll	10.0.19041.1	USB Performance Objects DLL
usbui.dll	10.0.19041.1	USB UI Dll
user32.dll	10.0.19041.488	Multi-User Windows USER API Client DLL
useraccountcontrolsettings.dll	10.0.19041.423	UserAccountControlSettings
useractivitybroker.dll	10.0.19041.388	useractivitybroker
usercpl.dll	10.0.19041.423	User control panel
userdataaccessres.dll	10.0.19041.1	Resource DLL for the UserDataAccess stack
userdataaccountapis.dll	10.0.19041.264	DLL for UserDataAccountsRT
userdatalanguageutil.dll	10.0.19041.1	Language-related helper functions for user data
userdataplatformhelperutil.dll	10.0.19041.1	Platform Utilities for data access
userdatatimeutil.dll	10.0.19041.488	Time-related helper functions for user data
userdatatypehelperutil.dll	10.0.19041.1	Type Utilities for data access
userdeviceregistration.dll	10.0.19041.388	AAD User Device Registration WinRT
userdeviceregistration.ngc.dll	10.0.19041.1	AD/AAD User Device Registration WinRT
userenv.dll	10.0.19041.1	Userenv
userinitext.dll	10.0.19041.1	UserInit Utility Extension DLL
userlanguageprofilecallback.dll	10.0.19041.1	MUI Callback for User Language profile changed
usermgrcli.dll	10.0.19041.1	UserMgr API DLL
usermgrproxy.dll	10.0.19041.1	UserMgrProxy
usoapi.dll	10.0.19041.388	Update Session Orchestrator API
usp10.dll	10.0.19041.1	Uniscribe Unicode script processor
ustprov.dll	10.0.19041.1	User State WMI Provider
utildll.dll	10.0.19041.1	WinStation utility support DLL
uudf.dll	10.0.19041.1	UDF Utility DLL
uxinit.dll	10.0.19041.1	Windows User Experience Session Initialization Dll
uxlib.dll	10.0.19041.1	Setup Wizard Framework

Navigation

uxlibres.dll	10.0.19041.1	UXLib Resources
uxtheme.dll	10.0.19041.488	Microsoft UxTheme Library
van.dll	10.0.19041.329	View Available Networks
vault.dll	10.0.19041.423	Windows vault Control Panel
vaultcli.dll	10.0.19041.264	Credential Vault Client Library
vbajet32.dll	6.0.1.9431	Visual Basic for Applications Development Environment - Expression Service Loader
vbscript.dll	5.812.10240.16384	Microsoft ® VBScript
vcamp110.dll	11.0.51106.1	Microsoft® C++ AMP Runtime
vcamp120.dll	12.0.40660.0	Microsoft® C++ AMP Runtime
vcamp140.dll	14.24.28127.4	Microsoft® C++ AMP Runtime
vcardparser.dll	10.0.19041.1	Supports the parsing of VCard and ICal formatted data
vccorlib110.dll	11.0.51106.1	Microsoft ® VC WinRT core library
vccorlib120.dll	12.0.40660.0	Microsoft ® VC WinRT core library
vccorlib140.dll	14.24.28127.4	Microsoft ® VC WinRT core library
vcomp100.dll	10.0.40219.325	Microsoft® C/C++ OpenMP Runtime
vcomp110.dll	11.0.51106.1	Microsoft® C/C++ OpenMP Runtime
vcomp120.dll	12.0.40660.0	Microsoft® C/C++ OpenMP Runtime
vcomp140.dll	14.24.28127.4	Microsoft® C/C++ OpenMP Runtime
vcruntime140.dll	14.24.28127.4	Microsoft® C Runtime Library
vcruntime140_clr0400.dll	14.10.25028.0	Microsoft® C Runtime Library
vdmdbg.dll	10.0.19041.1	VDMDBG.DLL
vds_ps.dll	10.0.19041.1	Microsoft® Virtual Disk Service proxy/stub
verifier.dll	10.0.19041.1	Standard application verifier provider dll
version.dll	10.0.19041.1	Version Checking and File Installation Libraries
vfwwdm32.dll	10.0.19041.1	VfW MM Driver for WDM Video Capture Devices
vidreszr.dll	10.0.19041.1	Windows Media Resizer
virtdisk.dll	10.0.19041.1	Virtual Disk API DLL
voiceactivationmanager.dll	10.0.19041.1	Windows Voice Activation Manager
voiprt.dll	10.0.19041.264	Voip Runtime
vpnikeapi.dll	10.0.19041.1	VPN IKE API's
vscmgrps.dll	10.0.19041.1	Microsoft Virtual Smart Card Manager Proxy/Stub
vss_ps.dll	10.0.19041.1	Microsoft® Volume Shadow Copy Service proxy/stub
vssapi.dll	10.0.19041.1	Microsoft® Volume Shadow Copy Requestor/Writer Services API DLL
vsstrace.dll	10.0.19041.1	Microsoft® Volume Shadow Copy Service Tracing Library
w32topl.dll	10.0.19041.1	Windows NT Topology Maintenance Tool
wab32.dll	10.0.19041.388	Microsoft (R) Contacts DLL
wab32.dll	10.0.19041.388	Microsoft (R) Contacts DLL
wab32res.dll	10.0.19041.388	Microsoft (R) Contacts DLL
wab32res.dll	10.0.19041.388	Microsoft (R) Contacts DLL
wabsyncprovider.dll	10.0.19041.1	Microsoft Windows Contacts Sync Provider
walletbackgroundserviceproxy.dll	10.0.19041.1	Wallet Background Proxy
walletproxy.dll	10.0.19041.1	Wallet proxy
wavemsp.dll	10.0.19041.329	Microsoft Wave MSP
wbemcomn.dll	10.0.19041.1	WMI
wcmapi.dll	10.0.19041.423	Windows Connection Manager Client API
wcnapi.dll	10.0.19041.1	Windows Connect Now - API Helper DLL
wcnwiz.dll	10.0.19041.1	Windows Connect Now Wizards
wdc.dll	10.0.19041.1	Performance Monitor
wdi.dll	10.0.19041.1	Windows Diagnostic Infrastructure
wdigest.dll	10.0.19041.388	Microsoft Digest Access
wdp.dll	10.0.19041.264	"wdp.DYNLINK"
wdscore.dll	10.0.19041.1	Panther Engine Module
webauthn.dll	10.0.19041.1	Web Authentication
webcamui.dll	10.0.19041.388	Microsoft® Windows® Operating System
webcheck.dll	11.0.19041.1	Web Site Monitor

Navigation

webclnt.dll	10.0.19041.1	Web DAV Service DLL
webio.dll	10.0.19041.1	Web Transfer Protocols API
webplatstorageserver.dll	10.0.19041.423	"webplatstorageserver.DYNLINK"
webservices.dll	10.0.19041.1	Windows Web Services Runtime
websocket.dll	10.0.19041.84	Web Socket API
wecapi.dll	10.0.19041.1	Event Collector Configuration API
wer.dll	10.0.19041.423	Windows Error Reporting DLL
werdiagcontroller.dll	10.0.19041.423	WER Diagnostic Controller
werenc.dll	10.0.19041.388	Windows Error Reporting Dump Encoding Library
weretw.dll	10.0.19041.423	WERETW.DLL
werui.dll	10.0.19041.388	Windows Error Reporting UI DLL
wevtapi.dll	10.0.19041.1	Eventing Consumption and Configuration API
wevtfwd.dll	10.0.19041.1	WS-Management Event Forwarding Plug-in
wfapigp.dll	10.0.19041.1	Windows Defender Firewall GPO Helper dll
wfdprov.dll	10.0.19041.488	Private WPS provisioning API DLL for Wi-Fi Direct
wfhc.dll	10.0.19041.1	Windows Defender Firewall Helper Class
whhelper.dll	10.0.19041.1	Net shell helper DLL for winHttp
wiaaut.dll	10.0.19041.329	WIA Automation Layer
wiadefui.dll	10.0.19041.1	WIA Scanner Default UI
wiadss.dll	10.0.19041.264	WIA TWAIN compatibility layer
wiascanprofiles.dll	10.0.19041.1	Microsoft Windows ScanProfiles
wiashext.dll	10.0.19041.1	Imaging Devices Shell Folder UI
wiatrace.dll	10.0.19041.21	WIA Tracing
wifidisplay.dll	10.0.19041.1	Wi-Fi Display DLL
wimgapi.dll	10.0.19041.423	Windows Imaging Library
win32u.dll	10.0.19041.508	Win32u
winbio.dll	10.0.19041.1	Windows Biometrics Client API
winbioext.dll	10.0.19041.1	Windows Biometrics Client Extension API
winbrand.dll	10.0.19041.1	Windows Branding Resources
wincorlib.dll	10.0.19041.508	Microsoft Windows ® WinRT core library
wincredprovider.dll	10.0.19041.1	wincredprovider DLL
wincredui.dll	10.0.19041.1	Credential Manager User Internal Interface
windowmanagementapi.dll		
windows.accountscontrol.dll	10.0.19041.488	Windows Accounts Control
windows.ai.machinelearning.dll	1.0.2007.1310	Windows Machine Learning Runtime
windows.ai.machinelearning.preview.dll	10.0.19041.264	WinRT Windows Machine Learning Preview DLL
windows.applicationmodel.background.systemeventsbroker.dll	10.0.19041.264	Windows Background System Events Broker API Server
windows.applicationmodel.background.timebroker.dll	10.0.19041.1	Windows Background Time Broker API Server
windows.applicationmodel.conversationalagent.dll	10.0.19041.423	Windows Voice Agent Services DLL
windows.applicationmodel.conversationalagent.internal.proxystub.dll		
windows.applicationmodel.conversationalagent.proxystub.dll		
windows.applicationmodel.core.dll	10.0.19041.388	Windows Application Model Core API
windows.applicationmodel.datatransfer.dll	10.0.19041.388	Windows.ApplicationModel.DataTransfer
windows.applicationmodel.dll	10.0.19041.388	Windows ApplicationModel API Server
windows.applicationmodel.lockscreen.dll	10.0.19041.388	Windows Lock Application Framework DLL
windows.applicationmodel.store.dll	10.0.19041.508	Microsoft Store Runtime DLL
windows.applicationmodel.store.preview.dosettings.dll	10.0.19041.1	Delivery Optimization Settings
windows.applicationmodel.store.testingframework.dll	10.0.19041.508	Microsoft Store Testing Framework Runtime DLL
windows.applicationmodel.wallet.dll	10.0.19041.264	Windows ApplicationModel Wallet Runtime DLL
windows.data.pdf.dll	10.0.19041.450	PDF WinRT APIs
windows.devices.alljoyn.dll	10.0.19041.388	Windows.Devices.AllJoyn DLL
windows.devices.background.dll	10.0.19041.1	Windows.Devices.Background
windows.devices.background.ps.dll	10.0.19041.1	Windows.Devices.Background Interface Proxy
windows.devices.bluetooth.dll	10.0.19041.388	Windows.Devices.Bluetooth DLL
windows.devices.custom.dll	10.0.19041.1	Windows.Devices.Custom

Navigation

windows.devices.custom.ps.dll	10.0.19041.1	Windows.Devices.Custom Interface Proxy
windows.devices.enumeration.dll	10.0.19041.388	Windows.Devices.Enumeration
windows.devices.haptics.dll	10.0.19041.264	Windows Runtime Haptics DLL
windows.devices.humaninterfacedevice.dll	10.0.19041.388	Windows.Devices.HumanInterfaceDevice DLL
windows.devices.lights.dll	10.0.19041.488	Windows Runtime Lights DLL
windows.devices.lowlevel.dll	10.0.19041.388	Windows.Devices.LowLevel DLL
windows.devices.midi.dll	10.0.19041.388	Windows Runtime MIDI Device server DLL
windows.devices.perception.dll	10.0.19041.388	Windows Devices Perception API
windows.devices.picker.dll	10.0.19041.388	Device Picker
windows.devices.pointofservice.dll	10.0.19041.388	Windows Runtime PointOfService DLL
windows.devices.portable.dll	10.0.19041.1	Windows Runtime Portable Devices DLL
windows.devices.printers.dll	10.0.19041.264	Windows Runtime Devices Printers DLL
windows.devices.printers.extensions.dll	10.0.19041.1	Windows.Devices.Printers.Extensions
windows.devices.radios.dll	10.0.19041.264	Windows.Devices.Radios DLL
windows.devices.scanners.dll	10.0.19041.264	Windows Runtime Devices Scanners DLL
windows.devices.sensors.dll	10.0.19041.388	Windows Runtime Sensors DLL
windows.devices.serialcommunication.dll	10.0.19041.388	Windows.Devices.SerialCommunication DLL
windows.devices.smartcards.dll	10.0.19041.388	Windows Runtime Smart Card API DLL
windows.devices.smartcards.phone.dll	10.0.19041.388	Windows Runtime Phone Smart Card Api DLL
windows.devices.usb.dll	10.0.19041.388	Windows Runtime Usb DLL
windows.devices.wifi.dll	10.0.19041.264	Windows.Devices.WiFi DLL
windows.devices.wifidirect.dll	10.0.19041.388	Windows.Devices.WiFiDirect DLL
windows.energy.dll	10.0.19041.388	Windows Energy Runtime DLL
windows.fileexplorer.common.dll	10.0.19041.423	Windows.FileExplorer.Common
windows.gaming.input.dll	10.0.19041.388	Windows Gaming Input API
windows.gaming.preview.dll	10.0.19041.388	Windows Gaming API Preview
windows.gaming.ui.gamebar.dll	10.0.19041.1	Windows Gaming UI API GameBar
windows.gaming.xboxlive.storage.dll	10.0.19041.264	Xbox Connected Storage WinRT implementation
windows.globalization.dll	10.0.19041.388	Windows Globalization
windows.globalization.fontgroups.dll	10.0.19041.1	Fonts Mapping API
windows.globalization.phonenumberformatting.dll	10.0.19041.1	Windows Libphonenumber OSS component
windows.graphics.display.brightnessoverride.dll	10.0.19041.264	Windows Runtime Brightness Override DLL
windows.graphics.display.displayenhancementoverride.dll	10.0.19041.1	Windows Runtime Display Enhancement Override DLL
windows.graphics.dll	10.0.19041.388	WinRT Windows Graphics DLL
windows.graphics.printing.3d.dll	10.0.19041.388	Microsoft Windows Printing Support
windows.graphics.printing.dll	10.0.19041.388	Microsoft Windows Printing Support
windows.graphics.printing.workflow.dll	10.0.19041.388	Microsoft Windows Print Workflow
windows.graphics.printing.workflow.native.dll	10.0.19041.388	Microsoft Windows Print Workflow Native
windows.internal.bluetooth.dll	10.0.19041.1	Windows.Internal.Bluetooth DLL
windows.internal.devices.sensors.dll	10.0.19041.388	Windows Runtime Sensors (Internal) DLL
windows.internal.graphics.display.displaycolormanagement.dll	10.0.19041.388	Windows Runtime Display Color Management DLL
windows.internal.graphics.display.displayenhancementmanagement.dll	10.0.19041.388	Windows Runtime Display Enhancement Management DLL
windows.internal.management.dll	10.0.19041.488	Windows Managent Service DLL
windows.internal.securitymitigationsbroker.dll	10.0.19041.1	Windows Security Mitigations Broker DLL
windows.internal.shellcommon.accountscontrolexperience.dll	10.0.19041.388	Shell Position default shell contract handler
windows.internal.shellcommon.printexperience.dll	10.0.19041.1	Print Experience default shell contract handler
windows.internal.shellcommon.tokenbrokermodal.dll	10.0.19041.1	Token broker default shell contract handler
windows.internal.ui.logon.proxystub.dll	10.0.19041.1	Logon User Experience Proxy Stub
windows.internal.ui.shell.windowtabmanager.dll		
windows.management.workplace.dll	10.0.19041.388	Windows Runtime MdmPolicy DLL
windows.management.workplace.workplacesettings.dll	10.0.19041.1	Windows Runtime WorkplaceSettings DLL
windows.media.audio.dll	10.0.19041.488	Windows Runtime Window Media Audio server DLL
windows.media.backgroundmediaplayback.dll	10.0.19041.1	Windows Media BackgroundMediaPlayback DLL
windows.media.devices.dll	10.0.19041.388	Windows Runtime media device server DLL
windows.media.dll	10.0.19041.388	Windows Media Runtime DLL

windows.media.editing.dll	10.0.19041.264	Windows Media Editing DLL
windows.media.faceanalysis.dll	10.0.19041.388	Microsoft (R) Face Detection DLL
windows.media.import.dll	10.0.19041.388	Windows Photo Import API (WinRT/COM)
windows.media.mediacontrol.dll	10.0.19041.388	Windows Runtime MediaControl server DLL
windows.media.mixedrealitycapture.dll	10.0.19041.1	"Windows.Media.MixedRealityCapture.DYNLINK"
windows.media.ocr.dll	10.0.19041.388	Windows OCR Runtime DLL
windows.media.playback.backgroundmediaplayer.dll	10.0.19041.1	Windows Media Playback BackgroundMediaPlayer DLL
windows.media.playback.mediaplayer.dll	10.0.19041.1	Windows Media Playback MediaPlayer DLL
windows.media.playback.proxystub.dll	10.0.19041.1	BackgroundMediaPlayer Proxy Stub DLL
windows.media.protection.playready.dll	10.0.19041.508	Microsoft PlayReady Client Framework Dll
windows.media.speech.dll	10.0.19041.388	Windows Speech Runtime DLL
windows.media.streaming.dll	10.0.19041.264	DLNA DLL
windows.media.streaming.ps.dll	10.0.19041.1	DLNA Proxy-Stub DLL
windows.mirage.dll	10.0.19041.1	Windows Perception API
windows.mirage.internal.dll	10.0.19041.1	"Windows.Mirage.Internal.DYNLINK"
windows.networking.backgroundtransfer.backgroundmanagerpolicy.dll	10.0.19041.1	Background Transfer Background Manager Policy DLL
windows.networking.backgroundtransfer.dll	10.0.19041.388	Windows.Networking.BackgroundTransfer DLL
windows.networking.connectivity.dll	10.0.19041.423	Windows Networking Connectivity Runtime DLL
windows.networking.dll	10.0.19041.264	Windows.Networking DLL
windows.networking.hostname.dll	10.0.19041.423	Windows.Networking.HostName DLL
windows.networking.networkoperators.esim.dll	10.0.19041.388	ESIM API
windows.networking.networkoperators.hotspotauthentication.dll	10.0.19041.1	Microsoft Windows Hotspot Authentication API
windows.networking.proximity.dll	10.0.19041.1	Windows Runtime Proximity API DLL
windows.networking.servicediscovery.dnssd.dll	10.0.19041.264	Windows.Networking.ServiceDiscovery.Dnssd DLL
windows.networking.sockets.pushenabledapplication.dll	10.0.19041.1	Windows.Networking.Sockets.PushEnabledApplication DLL
windows.networking.vpn.dll	10.0.19041.488	Windows.Networking.Vpn DLL
windows.networking.xboxlive.proxystub.dll	10.0.19041.1	Windows.Networking.XboxLive Proxy Stub Dll
windows.payments.dll	10.0.19041.508	Payment Windows Runtime DLL
windows.perception.stub.dll	10.0.19041.388	Windows Perception Api Stub
windows.security.authentication.identity.provider.dll	10.0.19041.388	Secondary Factor Authentication Windows Runtime DLL
windows.security.authentication.onlineid.dll	10.0.19041.423	Windows Runtime OnlineId Authentication DLL
windows.security.authentication.web.core.dll	10.0.19041.388	Token Broker WinRT API
windows.security.credentials.ui.credentialpicker.dll	10.0.19041.388	WinRT Credential Picker Server
windows.security.credentials.ui.userconsentverifier.dll	10.0.19041.264	Windows User Consent Verifier API
windows.security.integrity.dll	10.0.19041.1	Windows Lockdown API Server
windows.services.targetedcontent.dll	10.0.19041.388	Windows.Services.TargetedContent
windows.shell.servicehostbuilder.dll	10.0.19041.1	Windows.Shell.ServiceHostBuilder
windows.staterepository.dll	10.0.19041.508	Windows StateRepository API Server
windows.staterepositorybroker.dll	10.0.19041.508	Windows StateRepository API Broker
windows.staterepositoryclient.dll	10.0.19041.508	Windows StateRepository Client API
windows.staterepositorycore.dll	10.0.19041.508	Windows StateRepository API Core
windows.staterepositoryps.dll	10.0.19041.508	Windows StateRepository Proxy/Stub Server
windows.staterepositoryupgrade.dll	10.0.19041.508	Windows StateRepository Upgrade
windows.storage.applicationdata.dll	10.0.19041.388	Windows Application Data API Server
windows.storage.compression.dll	5.0.1.1	WinRT Compression
windows.storage.dll	10.0.19041.508	Microsoft WinRT Storage API
windows.storage.onecore.dll	10.0.19041.1	Microsoft Windows.Storage OneCore API
windows.storage.search.dll	10.0.19041.1	Windows.Storage.Search
windows.system.diagnostics.dll	10.0.19041.388	Windows System Diagnostics DLL
windows.system.diagnostics.telemetry.platformtelemetryclient.dll	10.0.19041.1	Platform Telemetry Client DLL
windows.system.diagnostics.tracereporting.platformdiagnosticactions.dll	10.0.19041.1	Platform Diagnostic Actions DLL
windows.system.launcher.dll	10.0.19041.488	Windows.System.Launcher
windows.system.profile.hardwareid.dll	10.0.19041.1	Windows System Profile HardwareId DLL
windows.system.profile.platformdiagnosticsandusagedatasettings.dll	10.0.19041.1	Platform Diagnostics and Usage Settings DLL
windows.system.profile.retailinfo.dll	10.0.19041.264	Windows.System.Profile.RetailInfo Runtime DLL

Navigation

Navigation

windows.system.profile.systemid.dll	10.0.19041.488	Windows System Profile SystemId DLL
windows.system.profile.systemmanufacturers.dll	10.0.19041.1	Windows.System.Profile.SystemManufacturers
windows.system.remotedesktop.dll	10.0.19041.1	Windows System RemoteDesktop Runtime DLL
windows.system.systemmanagement.dll	10.0.19041.264	Windows Runtime SystemManagement DLL
windows.system.userdeviceassociation.dll	10.0.19041.1	Windows System User Device Association API
windows.system.userprofile.diagnosticssettings.dll	10.0.19041.1	Diagnostics Settings DLL
windows.ui.accessibility.dll	10.0.19041.1	Windows.UI.Accessibility System DLL
windows.ui.core.textinput.dll	10.0.19041.508	Windows.UI.Core.TextInput dll
windows.ui.cred.dll	10.0.19041.1	Credential Prompt User Experience
windows.ui.creddialogcontroller.dll	10.0.19041.388	Credential UX Dialog Controller
windows.ui.dll	10.0.19041.264	Windows Runtime UI Foundation DLL
windows.ui.fileexplorer.dll	10.0.19041.488	Windows.UI.FileExplorer
windows.ui.immersive.dll	10.0.19041.450	WINDOWS.UI.IMMERSIVE
windows.ui.input.inking.analysis.dll	1.0.1907.3002	
windows.ui.input.inking.dll	10.0.19041.488	WinRT Windows Inking DLL
windows.ui.search.dll	10.0.19041.388	Windows.UI.Search
windows.ui.xaml.controls.dll	10.0.19041.1	Windows.UI.Xaml.Controls
windows.ui.xaml.dll	10.0.19041.488	Windows.UI.Xaml dll
windows.ui.xaml.inkcontrols.dll	10.0.19041.1	Windows UI XAML InkControls API
windows.ui.xaml.maps.dll	10.0.19041.264	Windows UI XAML Maps API
windows.ui.xaml.phone.dll	10.0.19041.1	Windows UI XAML Phone API
windows.ui.xamlhost.dll	10.0.19041.1	XAML Host
windows.web.diagnostics.dll	10.0.19041.1	Windows.Web.Diagnostics
windows.web.dll	10.0.19041.264	Web Client DLL
windows.web.http.dll	10.0.19041.264	Windows.Web.Http DLL
windowsaccessbridge-32.dll	8.0.2610.12	Java(TM) Platform SE binary
windowscodecs.dll	10.0.19041.388	Microsoft Windows Codecs Library
windowscodecsext.dll	10.0.19041.1	Microsoft Windows Codecs Extended Library
windowscodecsraw.dll	10.0.19041.508	Microsoft Camera Codec Pack
windowsdefaultheatprocessor.dll		
windowslivelogin.dll	10.0.19041.423	Microsoft® Account Login Helper
windowsperformancerecordercontrol.dll	10.0.19041.329	Microsoft Windows Performance Recorder Control Library
winfax.dll	10.0.19041.1	Microsoft Fax API Support DLL
winhttp.dll	10.0.19041.264	Windows HTTP Services
winhttpcom.dll	10.0.19041.1	Windows COM interface for WinHttp
wininet.dll	11.0.19041.508	Internet Extensions for Win32
wininetlui.dll	10.0.19041.1	Provides legacy UI for wininet
wininitext.dll	10.0.19041.1	WinInit Utility Extension DLL
winipcfile.dll	10.0.19041.1	Microsoft Active Directory Rights Management Services File API
winipcsecproc.dll	10.0.19041.1	Microsoft Active Directory Rights Management Services Desktop Security Processor
winipsec.dll	10.0.19041.1	Windows IPsec SPD Client DLL
winlangdb.dll	10.0.19041.1	Windows Bcp47 Language Database
winml.dll	10.0.19041.1	Windows Machine Learning Runtime
winmm.dll	10.0.19041.1	MCI API DLL
winmmbase.dll	10.0.19041.1	Base Multimedia Extension API DLL
winmsipc.dll	10.0.19041.1	Microsoft Active Directory Rights Management Services Client
winmsoirmprotector.dll	10.0.19041.1	Windows Office file format IRM Protector
winnlsres.dll	10.0.19041.1	NLSBuild resource DLL
winnsi.dll	10.0.19041.1	Network Store Information RPC interface
winopcirmprotector.dll	10.0.19041.1	Windows Office file format IRM Protector
winrnr.dll	10.0.19041.1	LDAP RnR Provider DLL
winrscmd.dll	10.0.19041.1	remtsvc
winrsmgr.dll	10.0.19041.1	WSMan Shell API
winrssrv.dll	10.0.19041.1	winrssrv
winrttracing.dll	10.0.19041.1	Windows Diagnostics Tracing

Navigation

winsatapi.dll	10.0.19041.207	Windows System Assessment Tool API
winscard.dll	10.0.19041.1	Microsoft Smart Card API
winshfhc.dll	10.0.19041.1	File Risk Estimation
winsku.dll	10.0.19041.1	Windows SKU Library
winsockhc.dll	10.0.19041.1	Winsock Network Diagnostic Helper Class
winsqlite3.dll	3.29.0.0	SQLite is a software library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.
winsrpc.dll	10.0.19041.1	WINS RPC LIBRARY
winsta.dll	10.0.19041.1	Winstation Library
winsync.dll	2007.94.19041.1	Synchronization Framework
winsyncmetastore.dll	2007.94.19041.1	Windows Synchronization Metadata Store
winsyncproviders.dll	2007.94.19041.1	Windows Synchronization Provider Framework
wintrust.dll	10.0.19041.423	Microsoft Trust Verification APIs
wintypes.dll	10.0.19041.508	Windows Base Types DLL
winusb.dll	10.0.19041.1	Windows USB Driver User Library
wisp.dll	10.0.19041.1	Microsoft Pen and Touch Input Component
wkscli.dll	10.0.19041.1	Workstation Service Client DLL
wkspbrokerax.dll	10.0.19041.329	Microsoft Workspace Broker ActiveX Control
wksprtps.dll	10.0.19041.1	WorkspaceRuntime ProxyStub DLL
wlanapi.dll	10.0.19041.488	Windows WLAN AutoConfig Client Side API DLL
wlancfg.dll	10.0.19041.488	Wlan Netsh Helper DLL
wlanconn.dll	10.0.19041.488	Dot11 Connection Flows
wlandlg.dll	10.0.19041.1	Wireless Lan Dialog Wizards
wlangpui.dll	10.0.19041.488	Wireless Network Policy Management Snap-in
wlanhlp.dll	10.0.19041.488	Windows Wireless LAN 802.11 Client Side Helper API
wlanmm.dll	10.0.19041.329	Dot11 Media and AdHoc Managers
wlanpref.dll	10.0.19041.1	Wireless Preferred Networks
wlanui.dll	10.0.19041.488	Wireless Profile UI
wlanutil.dll	10.0.19041.1	Windows Wireless LAN 802.11 Utility DLL
wldap32.dll	10.0.19041.1	Win32 LDAP API DLL
wldp.dll	10.0.19041.423	Windows Lockdown Policy
wlgpclnt.dll	10.0.19041.488	802.11 Group Policy Client
wlidcli.dll	10.0.19041.423	Microsoft® Account Dynamic Link Library
wlidcredprov.dll	10.0.19041.423	Microsoft® Account Credential Provider
wlidfdp.dll	10.0.19041.423	Microsoft® Account Function Discovery Provider
wlidnsp.dll	10.0.19041.423	Microsoft® Account Namespace Provider
wlidprov.dll	10.0.19041.423	Microsoft® Account Provider
wlidres.dll	10.0.19041.1	Microsoft® Windows Live ID Resource
wmadmod.dll	10.0.19041.508	Windows Media Audio Decoder
wmadmoe.dll	10.0.19041.508	Windows Media Audio 10 Encoder/Transcoder
wmasf.dll	12.0.19041.1	Windows Media ASF DLL
wmcodecdspps.dll	10.0.19041.1	Windows Media CodecDSP Proxy Stub Dll
wmdmlog.dll	12.0.19041.1	Windows Media Device Manager Logger
wmdmps.dll	12.0.19041.1	Windows Media Device Manager Proxy Stub
wmdrmsdk.dll	10.0.19041.1	WMDRM backwards compatibility stub
wmi.dll	10.0.19041.1	WMI DC and DP functionality
wmiclnt.dll	10.0.19041.1	WMI Client API
wmidcom.dll	10.0.19041.1	WMI
wmidx.dll	12.0.19041.329	Windows Media Indexer DLL
wmiprop.dll	10.0.19041.1	WDM Provider Dynamic Property Page CoInstaller
wmitomi.dll	10.0.19041.1	CIM Provider Adapter
wmnetmgr.dll	12.0.19041.329	Windows Media Network Plugin Manager DLL
wmphoto.dll	10.0.19041.1	Windows Media Photo Codec
wmsgapi.dll	10.0.19041.1	WinLogon IPC Client
wmspdmod.dll	10.0.19041.1	Windows Media Audio Voice Decoder

Navigation

wmspdmoe.dll	10.0.19041.508	Windows Media Audio Voice Encoder
wmvcore.dll	12.0.19041.488	Windows Media Playback/Authoring DLL
wmvdecod.dll	10.0.19041.450	Windows Media Video Decoder
wmvdspa.dll	10.0.19041.1	Windows Media Video DSP Components - Advanced
wmvencod.dll	10.0.19041.1	Windows Media Video 9 Encoder
wmvsdecd.dll	10.0.19041.1	Windows Media Screen Decoder
wmvsencd.dll	10.0.19041.1	Windows Media Screen Encoder
wmvxencd.dll	10.0.19041.1	Windows Media Video Encoder
wofutil.dll	10.0.19041.1	Windows Overlay File System Filter user mode API
wordbreakers.dll	10.0.19041.508	"WordBreakers.DYNLINK"
workfoldersres.dll	6.2.9200.16384	Work Folders Resources
wow32.dll	10.0.19041.423	Wow32
wpbcreds.dll	10.0.19041.1	WP 8.1 upgrade support utility
wpc.dll	10.0.19041.423	WPC Settings Library
wpcwebfilter.dll	10.0.19041.488	WpcWebFilter.dll
wpdshext.dll	10.0.19041.1	Portable Devices Shell Extension
wpdshserviceobj.dll	10.0.19041.1	Windows Portable Device Shell Service Object
wpdsp.dll	10.0.19041.1	WMDM Service Provider for Windows Portable Devices
wpnapps.dll	10.0.19041.450	Windows Push Notification Apps
wpnclient.dll	10.0.19041.388	Windows Push Notifications Client
wpportinglibrary.dll	10.0.19041.1	<d> DLL
ws2_32.dll	10.0.19041.1	Windows Socket 2.0 32-Bit DLL
ws2help.dll	10.0.19041.1	Windows Socket 2.0 Helper for Windows NT
wscapi.dll	10.0.19041.1	Windows Security Center API
wscinterop.dll	10.0.19041.1	Windows Health Center WSC Interop
wscisvif.dll	10.0.19041.1	Windows Security Center ISV API
wsclient.dll	10.0.19041.1	Microsoft Store Licensing Client
wscproxystub.dll	10.0.19041.1	Windows Security Center ISV Proxy Stub
wsdapi.dll	10.0.19041.1	Web Services for Devices API DLL
wsdchngr.dll	10.0.19041.1	WSD Challenge Component
wsecedit.dll	10.0.19041.488	Security Configuration UI Module
wshbth.dll	10.0.19041.1	Windows Sockets Helper DLL
wshcon.dll	5.812.10240.16384	Microsoft ® Windows Script Controller
wshelper.dll	10.0.19041.1	Winsock Net shell helper DLL for winsock
wshext.dll	5.812.10240.16384	Microsoft ® Shell Extension for Windows Script Host
wshhyperv.dll	10.0.19041.1	Hyper-V Winsock2 Helper DLL
wship6.dll	10.0.19041.1	Winsock2 Helper DLL (TL/IPv6)
wshqos.dll	10.0.19041.1	QoS Winsock2 Helper DLL
wshrm.dll	10.0.19041.1	Windows Sockets Helper DLL for PGM
wshtcpip.dll	10.0.19041.1	Winsock2 Helper DLL (TL/IPv4)
wshunix.dll	10.0.19041.1	AF_UNIX Winsock2 Helper DLL
wsmagent.dll	10.0.19041.488	WinRM Agent
wsmanmigrationplugin.dll	10.0.19041.488	WinRM Migration Plugin
wsmauto.dll	10.0.19041.488	WSMAN Automation
wsmplpxy.dll	10.0.19041.488	wsmplpxy
wsmres.dll	10.0.19041.488	WSMan Resource DLL
wsmsvc.dll	10.0.19041.488	WSMan Service
wsmwmipl.dll	10.0.19041.488	WSMAN WMI Provider
wsnmp32.dll	10.0.19041.1	Microsoft WinSNMP v2.0 Manager API
wsock32.dll	10.0.19041.1	Windows Socket 32-Bit DLL
wsp_fs.dll	10.0.19041.488	Windows Storage Provider for FileShare management
wsp_health.dll	10.0.19041.488	Windows Storage Provider for Health Agent API
wsp_sr.dll	10.0.19041.1	Windows Storage Provider for Storage Replication management
wtsapi32.dll	10.0.19041.1	Windows Remote Desktop Session Host Server SDK APIs
wuapi.dll	10.0.19041.508	Windows Update Client API

Navigation

wuceffects.dll	10.0.19041.1	Microsoft Composition Effects
wudriver.dll	10.0.19041.423	Windows Update WUDriver Stub
wups.dll	10.0.19041.488	Windows Update client proxy stub
wvc.dll	1.0.0.1	Windows Visual Components
wwaapi.dll	10.0.19041.264	Microsoft Web Application Host API library
wwaext.dll	10.0.19041.1	Microsoft Web Application Host Extension library
wwanapi.dll	10.0.19041.329	Mbnapi
wwapi.dll	10.0.19041.1	WWAN API
x3daudio1_0.dll	9.11.519.0	X3DAudio
xactengine2_1.dll	9.12.589.0	XACT Engine API
xactengine3_7.dll	9.29.1962.0	XACT Engine API
xapofx1_5.dll	9.29.1962.0	Audio Effect Library
xaudio2_7.dll	9.29.1962.0	XAudio2 Game Audio API
xaudio2_8.dll	10.0.19041.1	XAudio2 Game Audio API
xaudio2_9.dll	10.0.19041.1	XAudio2 Game Audio API
xblauthmanagerproxy.dll	10.0.19041.1	XblAuthManagerProxy
xblauthtokenbrokerext.dll	10.0.19041.1	Xbox Live Token Broker Extension
xblgamesaveproxy.dll	10.0.19041.1	Xbox Live Game Save Service Proxies and Stubs
xboxgipsynthetic.dll		
xinput1_1.dll	9.12.589.0	Microsoft Common Controller API
xinput1_4.dll	10.0.19041.1	Microsoft Common Controller API
xinput9_1_0.dll	10.0.19041.1	XNA Common Controller
xinputuap.dll	10.0.19041.1	Microsoft Common Controller API
xmlfilter.dll	2008.0.19041.1	XML Filter
xmllite.dll	10.0.19041.1	Microsoft XmlLite Library
xmlprovi.dll	10.0.19041.1	Network Provisioning Service Client API
xolehlp.dll	2001.12.10941.16384	Microsoft Distributed Transaction Coordinator Helper APIs DLL
xpsdocumenttargetprint.dll	10.0.19041.1	XPS DocumentTargetPrint DLL
xpsgdiconverter.dll	10.0.19041.1	XPS to GDI Converter
xpsprint.dll	10.0.19041.423	XPS Printing DLL
xpsrasterservice.dll	10.0.19041.1	XPS Rasterization Service Component
xpsservices.dll	10.0.19041.84	Xps Object Model in memory creation and deserialization
xwizards.dll	10.0.19041.1	Extensible Wizards Manager Module
xwreg.dll	10.0.19041.1	Extensible Wizard Registration Manager Module
xwtpdui.dll	10.0.19041.1	Extensible Wizard Type Plugin for DUI
xwtpw32.dll	10.0.19041.1	Extensible Wizard Type Plugin for Win32
zipcontainer.dll	10.0.19041.1	Zip Container DLL
zipfldr.dll	10.0.19041.1	Compressed (zipped) Folders
ztrace_maps.dll	10.0.19041.1	ZTrace Event Resources

Certificates

[Certificate Authorities / COMODO RSA Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA384 RSA (1.2.840.113549.1.1.12)
Serial Number	84 C0 D2 06 06 94 F5 4F E2 DA 7B F1 3E F4 DE 67
Validity	1/1/2004 - 1/1/2029
MD5 Hash	AB9B109CE8934F11E7CD22ED550680DA
SHA1 Hash	8D4C4A23BA9EE84EA7348FA98CC6E65FBB69DE7B

Navigation

Issuer Properties:

Common Name	AAA Certificate Services
Organization	Comodo CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Subject Properties:

Common Name	COMODO RSA Certification Authority
Organization	COMODO CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Microsoft Secure Server CA 2011]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	04 00 00 00 00 00 18 B7 3F 61
Validity	10/19/2011 - 10/19/2026
MD5 Hash	62455357DD57CB80C32AB295743CCCC0
SHA1 Hash	83DA05A9886F7658BE73ACF0A4930C0F99B92F01

Issuer Properties:

Common Name	Microsoft Root Certificate Authority 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Secure Server CA 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Microsoft Windows Hardware Compatibility]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	A0 69 FE 8F 9A 3F D1 11 8B 19
Validity	10/1/1997 - 12/31/2002
MD5 Hash	09C254BDE4EA50F26D1497F29C51AF6D
SHA1 Hash	109F1CAED645BB78B3EA2B94C0697C740733031C

Issuer Properties:

Navigation

Common Name	Microsoft Root Authority
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Corporation

Subject Properties:

Common Name	Microsoft Windows Hardware Compatibility
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Windows Hardware Compatibility Intermediate CA
Organizational Unit	Microsoft Corporation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Root Agency]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	F4 35 5C AA D4 B8 CF 11 8A 64 00 AA 00 6C 37 06
Validity	5/29/1996 - 1/1/2040
MD5 Hash	C0A723F0DA35026B21EDB17597F1D470
SHA1 Hash	FEE449EE0E3965A5246F000E87FDE2A065FD89D4

Issuer Properties:

Common Name	Root Agency

Subject Properties:

Common Name	Root Agency

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Sectigo RSA Domain Validation Secure Server CA]

Certificate Properties:

Version	V3
Signature Algorithm	SHA384 RSA (1.2.840.113549.1.1.12)
Serial Number	A7 0D 53 BC 0B 16 74 DB 11 BA 76 B4 26 51 5B 7D
Validity	11/2/2018 - 1/1/2031
MD5 Hash	ADAB5C4DF031FB9299F71ADA7E18F613
SHA1 Hash	33E4E80807204C2B6182A3A14B591ACD25B5F0DB

Issuer Properties:

Common Name	USERTrust RSA Certification Authority
Organization	The USERTRUST Network
Country	United States
Locality Name	Jersey City
State/Province	New Jersey

Subject Properties:

Common Name	Sectigo RSA Domain Validation Secure Server CA
Organization	Sectigo Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Navigation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Symantec Class 3 Extended Validation Code Signing CA - G2]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	49 7F 12 D5 8D 11 AC CF B8 97 9C 75 CB 32 1A 19
Validity	3/4/2014 - 3/4/2024
MD5 Hash	5CFFC3DED2AD28152293349639C54964
SHA1 Hash	5B8F88C80A73D35F76CD412A9E74E916594DFA67

Issuer Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	Symantec Class 3 Extended Validation Code Signing CA - G2
Organization	Symantec Corporation
Organizational Unit	Symantec Trust Network
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / thawte SHA256 Code Signing CA]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	CB 54 EE 18 9A 2B 3B C2 AF B1 DD 95 36 B7 A0 71
Validity	12/10/2013 - 12/10/2023
MD5 Hash	871953A98D4150C33C69A0C5AE9A68C6
SHA1 Hash	D00CFDBF46C98A838BC10DC4E097AE0152C461BC

Issuer Properties:

Common Name	thawte Primary Root CA
Organization	thawte, Inc.
Organizational Unit	Certification Services Division
Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	thawte SHA256 Code Signing CA
Organization	thawte, Inc.
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

Navigation

[Certificate Authorities / www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	8F 07 93 3F 23 98 60 92 0F 2F D0 B4 BA EB FC 46
Validity	4/17/1997 - 10/25/2016
MD5 Hash	ACD80EA27BB72CE700DC22724A5F1E92
SHA1 Hash	D559A586669B08F46A30A133F8A9ED3D038E2EA8

Issuer Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority
Country	United States

Subject Properties:

Organization	VeriSign Trust Network
Organizational Unit	VeriSign, Inc.
Organizational Unit	VeriSign International Server CA - Class 3

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[My Certificates / 55b896ab-52da-41c7-9bd0-6d6330adf3db]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	91 6E AF 16 96 27 5C 4C B0 65 9C 29 00 E2 35 61
Validity	9/8/2020 - 9/8/2030
MD5 Hash	9CC9A3E44EDD95C9A6AF9E373CC830F6
SHA1 Hash	59AD9B28644ECA19B3E5C05B1E444822CDD51537

Issuer Properties:

Common Name	MS-Organization-Access
Organizational Unit	82dbaca4-3e81-46ca-9c73-0950c1eaca97

Subject Properties:

Common Name	55b896ab-52da-41c7-9bd0-6d6330adf3db

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[My Certificates / APNS certificate Direct]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	A7 E7 C3 26 21 2C 2C BC 92 02
Validity	9/12/2020 - 9/12/2021
MD5 Hash	4C09CAEACF6B623952D61F1E45175BE5
SHA1 Hash	74BA8814D003F3FCE2AC45719D32F0D9EAD6B4B0

Navigation

Issuer Properties:

Common Name	Apple iPhone Device CA
Organization	Apple Inc.
Organizational Unit	Apple iPhone
Country	United States

Subject Properties:

Common Name	B456BE8E-03A4-467E-9922-E59931D8FB73

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Certum Trusted Network CA]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	C0 44 04
Validity	10/22/2008 - 12/31/2029
MD5 Hash	D5E98140C51869FC462C8975620FAA78
SHA1 Hash	07E032E020B72C3F192F0628A2593A19A70F069E

Issuer Properties:

Common Name	Certum Trusted Network CA
Organization	Unizeto Technologies S.A.
Organizational Unit	Certum Certification Authority
Country	Poland

Subject Properties:

Common Name	Certum Trusted Network CA
Organization	Unizeto Technologies S.A.
Organizational Unit	Certum Certification Authority
Country	Poland

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Certum]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	20 00 01
Validity	6/11/2002 - 6/11/2027
MD5 Hash	2C8F9F661D1890B147269D8E86828CA9
SHA1 Hash	6252DC40F71143A22FDE9EF7348E064251B18118

Issuer Properties:

Common Name	Certum CA
Organization	Unizeto Sp. z o.o.
Country	Poland

Subject Properties:

Common Name	Certum CA
Organization	Unizeto Sp. z o.o.

Country	Poland

Navigation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert Baltimore Root]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	B9 00 00 02
Validity	5/13/2000 - 5/13/2025
MD5 Hash	ACB694A59C17E0D791529BB19706A6E4
SHA1 Hash	D4DE20D05E66FC53FE1A50882C78DB2852CAE474

Issuer Properties:

Common Name	Baltimore CyberTrust Root
Organization	Baltimore
Organizational Unit	CyberTrust
Country	Ireland

Subject Properties:

Common Name	Baltimore CyberTrust Root
Organization	Baltimore
Organizational Unit	CyberTrust
Country	Ireland

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert Global Root G2]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	E5 FA 09 1D B1 64 28 BB A0 A9 11 A7 E6 F1 3A 03
Validity	8/1/2013 - 1/15/2038
MD5 Hash	E4A68AC854AC5242460AFD72481B2A44
SHA1 Hash	DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Issuer Properties:

Common Name	DigiCert Global Root G2
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert Global Root G2
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert Global Root G3]

Navigation

Certificate Properties:

Version	V3
Signature Algorithm	1.2.840.10045.4.3.3
Serial Number	72 45 AB D5 0F A4 C3 35 35 A4 5E F2 BC 56 55 05
Validity	8/1/2013 - 1/15/2038
MD5 Hash	F55DA450A5FB287E1E0F0DCC965756CA
SHA1 Hash	7E04DE896A3E666D00E687D33FFAD93BE83D349E

Issuer Properties:

Common Name	DigiCert Global Root G3
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert Global Root G3
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	1.2.840.10045.2.1

[Root Certificates / DigiCert]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	39 30 F0 1B FC 60 E5 8F FE 46 D8 17 E5 E0 E7 0C
Validity	11/10/2006 - 11/10/2031
MD5 Hash	87CE0B7B2A0E4900E158719B37A89372
SHA1 Hash	0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43

Issuer Properties:

Common Name	DigiCert Assured ID Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert Assured ID Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert]

Certificate Properties:

Version	V3

Navigation

Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	4A C7 91 59 C9 6A 75 A1 B1 46 42 90 56 E0 3B 08
Validity	11/10/2006 - 11/10/2031
MD5 Hash	79E4A9840D7D3A96D7C04FE2434C892E
SHA1 Hash	A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436

Issuer Properties:

Common Name	DigiCert Global Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert Global Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	77 25 46 AE F2 79 0B 8F 9B 40 0B 6A 26 5C AC 02
Validity	11/10/2006 - 11/10/2031
MD5 Hash	D474DE575C39B2D39C8583C5C065498A
SHA1 Hash	5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25

Issuer Properties:

Common Name	DigiCert High Assurance EV Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert High Assurance EV Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DST Root CA X3]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	6B 40 F8 2E 86 39 30 89 BA 27 A3 D6 80 B0 AF 44
Validity	10/1/2000 - 9/30/2021
MD5 Hash	410352DC0FF7501B16F0028EBA6F45C5
SHA1 Hash	DAC9024F54D8F6DF94935FB1732638CA6AD77C13

Navigation

Issuer Properties:

Common Name	DST Root CA X3
Organization	Digital Signature Trust Co.

Subject Properties:

Common Name	DST Root CA X3
Organization	Digital Signature Trust Co.

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Entrust (2048)]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	F8 DE 63 38
Validity	12/25/1999 - 7/24/2029
MD5 Hash	EE2931BC327E9AE6E8B5F751B4347190
SHA1 Hash	503006091D97D4F5AE39F7CBE7927D7D652D3431

Issuer Properties:

Common Name	Entrust.net Certification Authority (2048)
Organization	Entrust.net
Organizational Unit	www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
Organizational Unit	(c) 1999 Entrust.net Limited

Subject Properties:

Common Name	Entrust.net Certification Authority (2048)
Organization	Entrust.net
Organizational Unit	www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
Organizational Unit	(c) 1999 Entrust.net Limited

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Entrust]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	54 50 6B 45
Validity	11/28/2006 - 11/28/2026
MD5 Hash	D6A5C3ED5DDD3E00C13D87921F1D3FE4
SHA1 Hash	B31EB1B740E36C8402DADC37D44DF5D4674952F9

Issuer Properties:

Common Name	Entrust Root Certification Authority
Organization	Entrust, Inc.
Organizational Unit	www.entrust.net/CPS is incorporated by reference
Organizational Unit	(c) 2006 Entrust, Inc.
Country	United States

Subject Properties:

Navigation

Common Name	Entrust Root Certification Authority
Organization	Entrust, Inc.
Organizational Unit	www.entrust.net/CPS is incorporated by reference
Organizational Unit	(c) 2006 Entrust, Inc.
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GeoTrust Global CA]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	56 34 02
Validity	5/21/2002 - 5/21/2022
MD5 Hash	F775AB29FB514EB7775EFF053C998EF5
SHA1 Hash	DE28F4A4FFE5B92FA3C503D1A349A7F9962A8212

Issuer Properties:

Common Name	GeoTrust Global CA
Organization	GeoTrust Inc.
Country	United States

Subject Properties:

Common Name	GeoTrust Global CA
Organization	GeoTrust Inc.
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GlobalSign Root CA - R1]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	94 C3 5A 4B 15 01 00 00 00 00 04
Validity	9/1/1998 - 1/28/2028
MD5 Hash	3E455215095192E1B75D379FB187298A
SHA1 Hash	B1BC968BD4F49D622AA89A81F2150152A41D829C

Issuer Properties:

Common Name	GlobalSign Root CA
Organization	GlobalSign nv-sa
Organizational Unit	Root CA
Country	Belgium

Subject Properties:

Common Name	GlobalSign Root CA
Organization	GlobalSign nv-sa
Organizational Unit	Root CA
Country	Belgium

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

Navigation

[Root Certificates / GlobalSign Root CA - R3]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	A2 08 53 58 21 01 00 00 00 00 04
Validity	3/18/2009 - 3/18/2029
MD5 Hash	C5DFB849CA051355EE2DBA1AC33EB028
SHA1 Hash	D69B561148F01C77C54578C10926DF5B856976AD

Issuer Properties:

Common Name	GlobalSign
Organization	GlobalSign
Organizational Unit	GlobalSign Root CA - R3

Subject Properties:

Common Name	GlobalSign
Organization	GlobalSign
Organizational Unit	GlobalSign Root CA - R3

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Go Daddy Class 2 Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	00
Validity	6/30/2004 - 6/30/2034
MD5 Hash	91DE0625ABDAFD32170CBB25172A8467
SHA1 Hash	2796BAE63F1801E277261BA0D77770028F20EEE4

Issuer Properties:

Organization	The Go Daddy Group, Inc.
Organizational Unit	Go Daddy Class 2 Certification Authority
Country	United States

Subject Properties:

Organization	The Go Daddy Group, Inc.
Organizational Unit	Go Daddy Class 2 Certification Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Go Daddy Root Certificate Authority – G2]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)

Navigation

Serial Number	00
Validity	9/1/2009 - 1/1/2038
MD5 Hash	803ABC22C1E6FB8D9B3B274A321B9A01
SHA1 Hash	47BEABC922EAE80E78783462A79F45C254FDE68B

Issuer Properties:

Common Name	Go Daddy Root Certificate Authority - G2
Organization	GoDaddy.com, Inc.
Country	United States
Locality Name	Scottsdale
State/Province	Arizona

Subject Properties:

Common Name	Go Daddy Root Certificate Authority - G2
Organization	GoDaddy.com, Inc.
Country	United States
Locality Name	Scottsdale
State/Province	Arizona

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Google Trust Services - GlobalSign Root CA-R2]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	0D E6 26 86 0F 01 00 00 00 00 04
Validity	12/15/2006 - 12/15/2021
MD5 Hash	9414777E3E5EFD8F30BD41B0CFE7D030
SHA1 Hash	75E0ABB6138512271C04F85FDDDE38E4B7242EFE

Issuer Properties:

Common Name	GlobalSign
Organization	GlobalSign
Organizational Unit	GlobalSign Root CA - R2

Subject Properties:

Common Name	GlobalSign
Organization	GlobalSign
Organizational Unit	GlobalSign Root CA - R2

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Harmony(Test)]

Certificate Properties:

Version	V3
Signature Algorithm	1.3.14.3.2.29
Serial Number	55 1E 46 59 4C F6 C3 4D 8A E2 04 2C 60 AD FC 38
Validity	4/15/2010 - 1/1/2040
MD5 Hash	2E46CA54F8E41CAC8C05B0E69B5F3524
SHA1 Hash	0874A3219367D67070C0F6D15D8FB55E03AE581B

Navigation

Issuer Properties:

Common Name	Harmony(Test)

Subject Properties:

Common Name	Harmony(Test)

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / HarmonyNew(TEST)]

Certificate Properties:

Version	V3
Signature Algorithm	1.3.14.3.2.29
Serial Number	49 C0 23 46 B1 B8 63 48 8B E5 CD BE 73 A8 41 87
Validity	3/29/2011 - 1/1/2040
MD5 Hash	51380099AC3EFA39DDD0B2D555179FEC
SHA1 Hash	750F76D32AE307E5A87C42F5F86C7EAE69BE7120

Issuer Properties:

Common Name	HarmonyNew(TEST)

Subject Properties:

Common Name	HarmonyNew(TEST)

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Hotspot 2.0 Trust Root CA - 03]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	B7 ED 01 DE 89 09 B9 E0 33 A4 86 F2 70 0F B3 0C
Validity	12/8/2013 - 12/8/2043
MD5 Hash	EB1577B40B3C8BABAE346DD98EAD0780
SHA1 Hash	51501FBFCE69189D609CFAF140C576755DCC1FDF

Issuer Properties:

Common Name	Hotspot 2.0 Trust Root CA - 03
Organization	WFA Hotspot 2.0
Country	United States

Subject Properties:

Common Name	Hotspot 2.0 Trust Root CA - 03
Organization	WFA Hotspot 2.0
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Authenticode(tm) Root]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	01
Validity	1/1/1995 - 1/1/2000
MD5 Hash	DC6D6FAF897CDD17332FB5BA9035E9CE
SHA1 Hash	7F88CD7223F3C813818C994614A89C99FA3B5247

Issuer Properties:

Common Name	Microsoft Authenticode(tm) Root Authority
Organization	MSFT
Country	United States

Subject Properties:

Common Name	Microsoft Authenticode(tm) Root Authority
Organization	MSFT
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft ECC Product Root Certificate Authority 2018]

Certificate Properties:

Version	V3
Signature Algorithm	1.2.840.10045.4.3.3
Serial Number	85 EC 99 B9 7B 67 53 40 8F CD 7C DC 66 26 98 14
Validity	2/28/2018 - 2/28/2043
MD5 Hash	1F124EDE13E06A023CD7C09A4F48C3D6
SHA1 Hash	06F1AA330B927B753A40E68CDF22E34BCBEF3352

Issuer Properties:

Common Name	Microsoft ECC Product Root Certificate Authority 2018
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft ECC Product Root Certificate Authority 2018
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	1.2.840.10045.2.1

[Root Certificates / Microsoft ECC TS Root Certificate Authority 2018]

Certificate Properties:

Version	V3
Signature Algorithm	1.2.840.10045.4.3.3
Serial Number	45 82 12 41 AF EF B4 47 B0 D1 7E 64 E1 75 38 15
Validity	2/28/2018 - 2/28/2043
MD5 Hash	37942958862A06E6BBCFD7AB59C7F23C

SHA1 Hash	31F9FC8BA3805986B721EA7295C65B3A44534274

Navigation

Issuer Properties:

Common Name	Microsoft ECC TS Root Certificate Authority 2018
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft ECC TS Root Certificate Authority 2018
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	1.2.840.10045.2.1

[Root Certificates / Microsoft Root Authority]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	40 DF EC 63 F6 3E D1 11 88 3C 3C 8B 00 C1 00
Validity	1/10/1997 - 12/31/2020
MD5 Hash	2A954ECA79B2874573D92D90BAF99FB6
SHA1 Hash	A43489159A520F0D93D032CCAF37E7FE20A8B419

Issuer Properties:

Common Name	Microsoft Root Authority
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Corporation

Subject Properties:

Common Name	Microsoft Root Authority
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Corporation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Certificate Authority 2010]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	AA 39 43 6B 58 9B 9A 44 AC 44 BA BF 25 3A CC 28
Validity	6/24/2010 - 6/24/2035
MD5 Hash	A266BB7DCC38A562631361BBF61DD11B
SHA1 Hash	3B1EFD3A66EA28B16697394703A72CA340A05BD5

Issuer Properties:

Common Name	Microsoft Root Certificate Authority 2010
Organization	Microsoft Corporation

Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Root Certificate Authority 2010
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Certificate Authority 2011]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	44 E1 42 6C D6 69 B5 43 96 B2 9F FC B5 C8 8B 3F
Validity	3/23/2011 - 3/23/2036
MD5 Hash	CE0490D5E56C34A5AE0BE98BE581185D
SHA1 Hash	8F43288AD272F3103B6FB1428485EA3014C0BCFE

Issuer Properties:

Common Name	Microsoft Root Certificate Authority 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Root Certificate Authority 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Certificate Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	65 2E 13 07 F4 58 73 4C AD A5 A0 4A A1 16 AD 79
Validity	5/10/2001 - 5/10/2021
MD5 Hash	E1C07EA0AABBD4B77B84C228117808A7
SHA1 Hash	CDD4EEAE6000AC7F40C3802C171E30148030C072

Issuer Properties:

Common Name	Microsoft Root Certificate Authority

Subject Properties:

Common Name	Microsoft Root Certificate Authority

Navigation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Time Stamp Root Certificate Authority 2014]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	66 74 E2 3E 34 53 E9 45 90 32 93 22 43 7A D6 2F
Validity	10/23/2014 - 10/23/2039
MD5 Hash	34F72698D70E231F8DC45B57F118A44B
SHA1 Hash	0119E81BE9A14CD8E22F40AC118C687ECBA3F4D8

Issuer Properties:

Common Name	Microsoft Time Stamp Root Certificate Authority 2014
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Time Stamp Root Certificate Authority 2014
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Timestamp Root]

Certificate Properties:

Version	V1
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	01
Validity	5/13/1997 - 12/31/1999
MD5 Hash	556EBEF54C1D7C0360C43418BC9649C1
SHA1 Hash	245C97DF7514E7CF2DF8BE72AE957B9E04741E85

Issuer Properties:

Organization	Microsoft Trust Network
Organizational Unit	Microsoft Corporation
Organizational Unit	Microsoft Time Stamping Service Root

Subject Properties:

Organization	Microsoft Trust Network
Organizational Unit	Microsoft Corporation
Organizational Unit	Microsoft Time Stamping Service Root

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

Navigation

[Root Certificates / QuoVadis Root Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	8B 50 B6 3A
Validity	3/20/2001 - 3/18/2021
MD5 Hash	27DE36FE72B70003009DF4F01E6C0424
SHA1 Hash	DE3F40BD5093D39B6C60F6DABC076201008976C9

Issuer Properties:

Common Name	QuoVadis Root Certification Authority
Organization	QuoVadis Limited
Organizational Unit	Root Certification Authority
Country	Bermuda

Subject Properties:

Common Name	QuoVadis Root Certification Authority
Organization	QuoVadis Limited
Organizational Unit	Root Certification Authority
Country	Bermuda

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / SECOM Trust Systems Co Ltd.]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	00
Validity	5/29/2009 - 5/29/2029
MD5 Hash	6C397DA40E5559B23FD641B11250DE43
SHA1 Hash	5F3B8CF2F810B37D78B4CEEC1919C37334B9C774

Issuer Properties:

Organization	SECOM Trust Systems CO.,LTD.
Organizational Unit	Security Communication RootCA2
Country	Japan

Subject Properties:

Organization	SECOM Trust Systems CO.,LTD.
Organizational Unit	Security Communication RootCA2
Country	Japan

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / SECOM Trust Systems CO LTD]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)

Serial Number	00
Validity	9/30/2003 - 9/30/2023
MD5 Hash	F1BC636A54E0B527F5CDE71AE34D6E4A
SHA1 Hash	36B12B49F9819ED74C9EBC380FC6568F5DACB2F7

Issuer Properties:

Organization	SECOM Trust.net
Organizational Unit	Security Communication RootCA1
Country	Japan

Subject Properties:

Organization	SECOM Trust.net
Organizational Unit	Security Communication RootCA1
Country	Japan

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Sectigo (AAA)]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	01
Validity	1/1/2004 - 1/1/2029
MD5 Hash	497904B0EB8719AC47B0BC11519B74D0
SHA1 Hash	D1EB23A46D17D68FD92564C2F1F1601764D8E349

Issuer Properties:

Common Name	AAA Certificate Services
Organization	Comodo CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Subject Properties:

Common Name	AAA Certificate Services
Organization	Comodo CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Sectigo (AddTrust)]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	01
Validity	5/30/2000 - 5/30/2020
MD5 Hash	1D3554048578B03F42424DBF20730A3F
SHA1 Hash	02FAF3E291435468607857694DF5E45B68851868

Navigation

Issuer Properties:

Common Name	AddTrust External CA Root
Organization	AddTrust AB
Organizational Unit	AddTrust External TTP Network
Country	Sweden

Subject Properties:

Common Name	AddTrust External CA Root
Organization	AddTrust AB
Organizational Unit	AddTrust External TTP Network
Country	Sweden

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Sectigo (formerly Comodo CA)]

Certificate Properties:

Version	V3
Signature Algorithm	SHA384 RSA (1.2.840.113549.1.1.12)
Serial Number	9D 86 03 5B D8 4E F7 1F E0 6F 63 DB CA F9 AA 4C
Validity	1/19/2010 - 1/19/2038
MD5 Hash	1B31B0714036CC143691ADC43EFDEC18
SHA1 Hash	AFE5D244A8D1194230FF479FE2F897BBCD7A8CB4

Issuer Properties:

Common Name	COMODO RSA Certification Authority
Organization	COMODO CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Subject Properties:

Common Name	COMODO RSA Certification Authority
Organization	COMODO CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Sectigo]

Certificate Properties:

Version	V3
Signature Algorithm	SHA384 RSA (1.2.840.113549.1.1.12)
Serial Number	2D 03 35 0E 64 BC 1B A8 51 CA A3 FC 30 6D FD 01
Validity	2/1/2010 - 1/19/2038
MD5 Hash	1BFE69D191B71933A372A80FE155E5B5
SHA1 Hash	2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E

Issuer Properties:

Common Name	USERTrust RSA Certification Authority
Organization	The USERTRUST Network

Navigation

Country	United States
Locality Name	Jersey City
State/Province	New Jersey

Subject Properties:

Common Name	USERTrust RSA Certification Authority
Organization	The USERTRUST Network
Country	United States
Locality Name	Jersey City
State/Province	New Jersey

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Starfield Class 2 Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	00
Validity	6/30/2004 - 6/30/2034
MD5 Hash	324A4BBBC863699BBE749AC6DD1D4624
SHA1 Hash	AD7E1C28B064EF8F6003402014C3D0E3370EB58A

Issuer Properties:

Organization	Starfield Technologies, Inc.
Organizational Unit	Starfield Class 2 Certification Authority
Country	United States

Subject Properties:

Organization	Starfield Technologies, Inc.
Organizational Unit	Starfield Class 2 Certification Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Symantec Enterprise Mobile Root for Microsoft]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	CE D8 F4 BD A9 29 66 0F 7B 90 BF 9E 2F 55 6B 0F
Validity	3/15/2012 - 3/15/2032
MD5 Hash	71D0A5FF2D59741694BEE37D1E5C860B
SHA1 Hash	92B46C76E13054E104F230517E6E504D43AB10B5

Issuer Properties:

Common Name	Symantec Enterprise Mobile Root for Microsoft
Organization	Symantec Corporation
Country	United States

Subject Properties:

Common Name	Symantec Enterprise Mobile Root for Microsoft

Organization	Symantec Corporation
Country	United States

Navigation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Thawte Timestamping CA]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	00
Validity	1/1/1997 - 1/1/2021
MD5 Hash	7F667A71D3EB6978209A51149D83DA20
SHA1 Hash	BE36A4562FB2EE05DBB3D32323ADF445084ED656

Issuer Properties:

Common Name	Thawte Timestamping CA
Organization	Thawte
Organizational Unit	Thawte Certification
Country	South Africa
Locality Name	Durbanville
State/Province	Western Cape

Subject Properties:

Common Name	Thawte Timestamping CA
Organization	Thawte
Organizational Unit	Thawte Certification
Country	South Africa
Locality Name	Durbanville
State/Province	Western Cape

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / thawte]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	6D 2B DB 37 CE 2F F4 49 EC ED D5 20 57 D5 4E 34
Validity	11/17/2006 - 7/17/2036
MD5 Hash	8CCADC0B22CEF5BE72AC411A11A8D812
SHA1 Hash	91C6D6EE3E8AC86384E548C299295C756C817B81

Issuer Properties:

Common Name	thawte Primary Root CA
Organization	thawte, Inc.
Organizational Unit	Certification Services Division
Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	thawte Primary Root CA
Organization	thawte, Inc.

Organizational Unit	Certification Services Division
Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign Class 3 Public Primary CA]

Certificate Properties:

Version	V1
Signature Algorithm	MD2 RSA (1.2.840.113549.1.1.2)
Serial Number	BF BA CC 03 7B CA 38 B6 34 29 D9 10 1D E4 BA 70
Validity	1/29/1996 - 8/2/2028
MD5 Hash	10FC635DF6263E0DF325BE5F79CD6767
SHA1 Hash	742C3192E607E424EB4549542BE1BBC53E6174E2

Issuer Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority
Country	United States

Subject Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign Time Stamping CA]

Certificate Properties:

Version	V1
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	A3 DC 5D 15 5F 73 5D A5 1C 59 82 8C 38 D2 19 4A
Validity	5/12/1997 - 1/8/2004
MD5 Hash	EBB04F1D3A2E372F1DDA6E27D6B680FA
SHA1 Hash	18F7C1FCC3090203FD5BAA2F861A754976C8DD25

Issuer Properties:

Organization	VeriSign Trust Network
Organizational Unit	VeriSign, Inc.
Organizational Unit	VeriSign Time Stamping Service Root
Organizational Unit	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.

Subject Properties:

Organization	VeriSign Trust Network
Organizational Unit	VeriSign, Inc.
Organizational Unit	VeriSign Time Stamping Service Root
Organizational Unit	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign Universal Root Certification Authority]

Navigation

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	1D C5 1A 12 E4 BB 0E 03 21 13 B3 21 64 C4 1A 40
Validity	4/2/2008 - 12/2/2037
MD5 Hash	8EADB501AA4D81E48C1DD1E114009519
SHA1 Hash	3679CA35668772304D30A5FB873B0FA77BB70D54

Issuer Properties:

Common Name	VeriSign Universal Root Certification Authority
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2008 VeriSign, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	VeriSign Universal Root Certification Authority
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2008 VeriSign, Inc. - For authorized use only
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	4A 3B 6B CC CD 58 21 4A BB E8 7D 26 9E D1 DA 18
Validity	11/8/2006 - 7/17/2036
MD5 Hash	CB17E431673EE209FE455793F30AFA1C
SHA1 Hash	4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5

Issuer Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

UpTime

Current Session:

Last Shutdown Time	9/12/2020 8:22:50 PM
Last Boot Time	9/12/2020 8:48:13 PM
Last DownTime	1523 sec (0 days, 0 hours, 25 min, 23 sec)
Current Time	9/12/2020 9:11:42 PM
UpTime	1409 sec (0 days, 0 hours, 23 min, 29 sec)

UpTime Statistics:

First Boot Time	9/8/2020 11:54:23 AM
First Shutdown Time	9/8/2020 11:57:28 AM
Total UpTime	157451 sec (1 days, 19 hours, 44 min, 11 sec)
Total DownTime	221588 sec (2 days, 13 hours, 33 min, 8 sec)
Longest UpTime	55947 sec (0 days, 15 hours, 32 min, 27 sec)
Longest DownTime	66024 sec (0 days, 18 hours, 20 min, 24 sec)
Total Reboots	15
System Availability	41.54%

Bluescreen Statistics:

First Bluescreen Time	9/9/2020 5:51:45 PM
Last Bluescreen Time	9/11/2020 11:39:46 AM
Total Bluescreens	3

Information:

Information	The above statistics are based on System Event Log entries

Share

Share Name	Type	Remark	Local Path
ADMIN$	Folder	Remote Admin	C:\WINDOWS
C$	Folder	Default share	C:\
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]

Account Security

Account Security Properties:

Computer Role	Primary
Domain Name	VIETHOANG
Primary Domain Controller	Not Specified
Forced Logoff Time	Disabled
Min / Max Password Age	0 / 42 days
Minimum Password Length	0 chars
Password History Length	Disabled
Lockout Threshold	Disabled
Lockout Duration	30 min
Lockout Observation Window	30 min

Navigation

Logon

User	Full Name	Logon Server	Logon Domain
bebosmj0@gmail.com			MicrosoftAccount
bebosmj0@gmail.com			MicrosoftAccount

Users

[Administrator]

User Properties:

User Name	Administrator
Full Name	Administrator
Comment	Built-in account for administering the computer/domain
Member Of Groups	Administrators
Logon Count	0
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	Yes
Locked Out User	No
Home Folder Required	No
Password Required	Yes
Read-Only Password	No
Password Never Expires	Yes

[bebos]

User Properties:

User Name	bebos
Full Name	Bé Bo
Member Of Groups	Administrators; Users
Logon Count	0
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	No
Locked Out User	No
Home Folder Required	No
Password Required	Yes
Read-Only Password	No
Password Never Expires	Yes

[DefaultAccount]

User Properties:

Navigation

User Name	DefaultAccount
Full Name	DefaultAccount
Comment	A user account managed by the system.
Member Of Groups	System Managed Accounts Group
Logon Count	0
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	Yes
Locked Out User	No
Home Folder Required	No
Password Required	No
Read-Only Password	No
Password Never Expires	Yes

[Guest]

User Properties:

User Name	Guest
Full Name	Guest
Comment	Built-in account for guest access to the computer/domain
Member Of Groups	Guests
Logon Count	0
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	Yes
Locked Out User	No
Home Folder Required	No
Password Required	No
Read-Only Password	Yes
Password Never Expires	Yes

[WDAGUtilityAccount]

User Properties:

User Name	WDAGUtilityAccount
Full Name	WDAGUtilityAccount
Comment	A user account managed and used by the system for Windows Defender Application Guard scenarios.
Logon Count	0
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	Yes
Locked Out User	No
Home Folder Required	No
Password Required	Yes
Read-Only Password	No
Password Never Expires	No

Local Groups

Navigation

[Access Control Assistance Operators]

Local Group Properties:

Comment	Members of this group can remotely query authorization attributes and permissions for resources on this computer.

[Administrators]

Local Group Properties:

Comment	Administrators have complete and unrestricted access to the computer/domain

Group Members:

Administrator	
bebos	Bé Bo

[Backup Operators]

Local Group Properties:

Comment	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files

[Cryptographic Operators]

Local Group Properties:

Comment	Members are authorized to perform cryptographic operations.

[Device Owners]

Local Group Properties:

Comment	Members of this group can change system-wide settings.

[Distributed COM Users]

Local Group Properties:

Comment	Members are allowed to launch, activate and use Distributed COM objects on this machine.

[Event Log Readers]

Local Group Properties:

Comment	Members of this group can read event logs from local machine

[Guests]

Local Group Properties:

Comment	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted

Group Members:

Guest	

[Hyper-V Administrators]

Local Group Properties:
Comment Members of this group have complete and unrestricted access to all features of Hyper-V.

Navigation

[IIS_IUSRS]

Local Group Properties:
Comment Built-in group used by Internet Information Services.

Group Members:
IUSR

[Network Configuration Operators]

Local Group Properties:
Comment Members in this group can have some administrative privileges to manage configuration of networking features

[Performance Log Users]

Local Group Properties:
Comment Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer

[Performance Monitor Users]

Local Group Properties:
Comment Members of this group can access performance counter data locally and remotely

[Power Users]

Local Group Properties:
Comment Power Users are included for backwards compatibility and possess limited administrative powers

[Remote Desktop Users]

Local Group Properties:
Comment Members in this group are granted the right to logon remotely

[Remote Management Users]

Local Group Properties:
Comment Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

[Replicator]

Local Group Properties:
Comment Supports file replication in a domain

[System Managed Accounts Group]

Local Group Properties:
Comment Members of this group are managed by the system.

Group Members:

DefaultAccount

Navigation

[Users]

Local Group Properties:

Comment	Users are prevented from making accidental or intentional system-wide changes and can run most applications

Group Members:

Authenticated Users	
bebos	Bé Bo
INTERACTIVE	

Global Groups

[None]

Global Group Properties:

Comment	Ordinary users

Group Members:

Administrator	
bebos	Bé Bo
DefaultAccount	
Guest	
WDAGUtilityAccount	

Windows Video

[Intel(R) HD Graphics 2500]

Video Adapter Properties:

Device Description	Intel(R) HD Graphics 2500
Adapter String	Intel(R) HD Graphics 2500
BIOS String	Intel Video BIOS
Chip Type	Intel(R) HD Graphics Family
DAC Type	Internal
Driver Date	1/21/2020
Driver Version	10.18.10.5129
Driver Provider	Intel Corporation
Memory Size	2097650 KB

Installed Drivers:

igdumdim64	10.18.10.5129
igd10iumd64	10.18.10.5129
igd10iumd64	10.18.10.5129
igdumdim32	10.18.10.5129
igd10iumd32	10.18.10.5129
igd10iumd32	10.18.10.5129

Navigation

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Intel(R) HD Graphics 2500]

Video Adapter Properties:

Device Description	Intel(R) HD Graphics 2500
Adapter String	Intel(R) HD Graphics 2500
BIOS String	Intel Video BIOS
Chip Type	Intel(R) HD Graphics Family
DAC Type	Internal
Driver Date	1/21/2020
Driver Version	10.18.10.5129
Driver Provider	Intel Corporation
Memory Size	2097650 KB

Installed Drivers:

igdumdim64	10.18.10.5129
igd10iumd64	10.18.10.5129
igd10iumd64	10.18.10.5129
igdumdim32	10.18.10.5129
igd10iumd32	10.18.10.5129
igd10iumd32	10.18.10.5129

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Intel(R) HD Graphics 2500]

Video Adapter Properties:

Device Description	Intel(R) HD Graphics 2500
Adapter String	Intel(R) HD Graphics 2500
BIOS String	Intel Video BIOS
Chip Type	Intel(R) HD Graphics Family
DAC Type	Internal
Driver Date	1/21/2020
Driver Version	10.18.10.5129
Driver Provider	Intel Corporation
Memory Size	2097650 KB

Installed Drivers:

igdumdim64	10.18.10.5129
igd10iumd64	10.18.10.5129
igd10iumd64	10.18.10.5129
igdumdim32	10.18.10.5129
igd10iumd32	10.18.10.5129
igd10iumd32	10.18.10.5129

Navigation

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

PCI / AGP Video

Device Description	Device Type
Intel HD Graphics 2500	Video Adapter
Intel HD Graphics 2500	3D Accelerator

GPU

[Integrated: Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)]

Graphics Processor Properties:

Video Adapter	Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)
BIOS Version	Build Number: 2132Ta PC 14.34 02/13/2012 11:14:00
BIOS Date	2/13/2012
GPU Code Name	Ivy Bridge-DT GT1
PCI Device	8086-0152 / 10CF-176D (Rev 09)
Process Technology	22 nm
Bus Type	Integrated
GPU Clock	349 MHz (original: 649 MHz)
GPU Clock (Turbo)	349 - 1048 MHz
RAMDAC Clock	350 MHz
Pixel Pipelines	4
TMU Per Pipeline	1
Unified Shaders	24 (v5.0)
DirectX Hardware Support	DirectX v11.1
WDDM Version	WDDM 1.3

Architecture:

Architecture	Intel Gen7
Execution Units (EU)	6
L1 Instruction Cache	32 KB
L1 Texture Cache	4 KB
L2 Texture Cache	24 KB
L3 Cache	128 KB
Unified Return Buffer	128 KB

Theoretical Peak Performance:

Pixel Fillrate	1396 MPixel/s @ 349 MHz
Texel Fillrate	[TRIAL VERSION]
Single-Precision FLOPS	33.5 GFLOPS @ 349 MHz
Double-Precision FLOPS	[TRIAL VERSION]

Utilization:

Dedicated Memory	12 MB

Dynamic Memory	109 MB

Navigation

Graphics Processor Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Monitor

[Samsung SyncMaster E1920/E1920X/EX1920/EX1920X (Analog)]

Monitor Properties:

Monitor Name	Samsung SyncMaster E1920/E1920X/EX1920/EX1920X (Analog)
Monitor ID	SAM06B7
Model	SME1920
Monitor Type	19" LCD (WXGA)
Manufacture Date	Week 35 / 2010
Serial Number	HDBZ824304
Max. Visible Display Size	410 mm x 230 mm (18.5")
Picture Aspect Ratio	16:9
Horizontal Frequency	30 - 81 kHz
Vertical Frequency	56 - 75 Hz
Maximum Pixel Clock	90 MHz
Maximum Resolution	1360 x 768
Pixel Density	84 ppi
Gamma	2.20
DPMS Mode Support	Active-Off

Supported Video Modes:

640 x 480	60 Hz
640 x 480	67 Hz
640 x 480	72 Hz
640 x 480	75 Hz
720 x 400	70 Hz
800 x 600	56 Hz
800 x 600	60 Hz
800 x 600	72 Hz
800 x 600	75 Hz
832 x 624	75 Hz
1024 x 768	60 Hz
1024 x 768	72 Hz
1024 x 768	75 Hz
1366 x 768	Pixel Clock: 85.50 MHz

Monitor Manufacturer:

Company Name	Samsung
Product Information	http://www.samsung.com/us/computer/monitors
Driver Download	http://www.samsung.com/us/support
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Desktop

Navigation

Desktop Properties:

Device Technology	Raster Display
Resolution	1360 x 768
Color Depth	32-bit
Color Planes	1
Font Resolution	96 dpi
Taskbar Button Combining	Always, hide labels
Pixel Width / Height	36 / 36
Pixel Diagonal	51
Vertical Refresh Rate	60 Hz
Desktop Wallpaper	c:\users\bebos\appdata\local\microsoft\windows\themes\roamedthemefiles\desktopbackground\img0.jpg

Desktop Effects:

Combo-Box Animation	Enabled
Dark Mode	Disabled
Drop Shadow Effect	Enabled
Flat Menu Effect	Enabled
Font Smoothing	Enabled
ClearType	Enabled
Full Window Dragging	Enabled
Gradient Window Title Bars	Enabled
Hide Menu Access Keys	Enabled
Hot Tracking Effect	Enabled
Icon Title Wrapping	Enabled
List-Box Smooth Scrolling	Enabled
Menu Animation	Enabled
Menu Fade Effect	Enabled
Minimize/Restore Animation	Enabled
Mouse Cursor Shadow	Disabled
Selection Fade Effect	Enabled
ShowSounds Accessibility Feature	Disabled
Small Taskbar Buttons	Disabled
Taskbar Button Badges	Enabled
Taskbar Locked	Yes
ToolTip Animation	Enabled
ToolTip Fade Effect	Enabled
Windows Aero	Enabled
Windows Plus! Extension	Disabled

Multi-Monitor

Device ID	Primary	Upper Left Corner	Bottom Right Corner
\\.\DISPLAY1	Yes	(0,0)	(1360,768)

Video Modes

Navigation

Resolution	Color Depth	Refresh Rate
320 x 200	32-bit	60 Hz
320 x 200	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
320 x 240	32-bit	60 Hz
320 x 240	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
400 x 300	32-bit	60 Hz
400 x 300	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
512 x 384	32-bit	60 Hz
512 x 384	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
640 x 400	32-bit	60 Hz
640 x 400	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
640 x 400	32-bit	70 Hz
640 x 480	32-bit	59 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
640 x 480	32-bit	60 Hz
640 x 480	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
640 x 480	32-bit	73 Hz
640 x 480	32-bit	75 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
800 x 600	32-bit	60 Hz
800 x 600	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
800 x 600	32-bit	75 Hz
1024 x 768	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
1024 x 768	32-bit	60 Hz
1024 x 768	32-bit	70 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
1280 x 600	32-bit	60 Hz
1280 x 600	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
1280 x 720	32-bit	60 Hz
1280 x 720	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
1280 x 768	32-bit	60 Hz
1280 x 768	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
1360 x 768	32-bit	60 Hz
1360 x 768	32-bit	60 Hz
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
1366 x 768	32-bit	60 Hz

OpenGL

OpenGL Properties:

Vendor	Intel
Renderer	Intel(R) HD Graphics 2500

Version	4.0.0 - Build 10.18.10.5129
Shading Language Version	4.00 - Build 10.18.10.5129
OpenGL DLL	10.0.19041.488(WinBuild.160101.0800)
Multitexture Texture Units	8
Occlusion Query Counter Bits	64
Sub-Pixel Precision	4-bit
Max Viewport Size	16384 x 16384
Max Cube Map Texture Size	16384 x 16384
Max Rectangle Texture Size	16384 x 16384
Max 3D Texture Size	2048 x 2048 x 2048
Max Anisotropy	16
Max Clipping Planes	8
Max Display-List Nesting Level	64
Max Draw Buffers	8
Max Evaluator Order	32
Max Light Sources	8
Max Pixel Map Table Size	65536
Min / Max Program Texel Offset	-8 / 7
Max Texture Array Layers	2048
Max Texture LOD Bias	15

OpenGL Compliancy:

OpenGL 1.1	Yes (100%)
OpenGL 1.2	Yes (100%)
OpenGL 1.3	Yes (100%)
OpenGL 1.4	Yes (100%)
OpenGL 1.5	Yes (100%)
OpenGL 2.0	Yes (100%)
OpenGL 2.1	Yes (100%)
OpenGL 3.0	Yes (100%)
OpenGL 3.1	Yes (100%)
OpenGL 3.2	Yes (100%)
OpenGL 3.3	Yes (100%)
OpenGL 4.0	Yes (100%)
OpenGL 4.1	No (85%)
OpenGL 4.2	No (83%)
OpenGL 4.3	No (42%)
OpenGL 4.4	No (11%)
OpenGL 4.5	No (0%)
OpenGL 4.6	No (0%)

Max Stack Depth:

Attribute Stack	16
Client Attribute Stack	16
Modelview Matrix Stack	32
Name Stack	128
Projection Matrix Stack	4
Texture Matrix Stack	10

Draw Range Elements:

Max Index Count	1048576
Max Vertex Count	1048576

Transform Feedback:

Max Interleaved Components	128

Max Separate Attributes	4
Max Separate Components	4

Navigation

Framebuffer Object:

Max Color Attachments	8
Max Render Buffer Size	16384 x 16384

Vertex Shader:

Max Uniform Vertex Components	4096
Max Varying Floats	64
Max Vertex Texture Image Units	16
Max Combined Texture Image Units	96

Geometry Shader:

Max Geometry Texture Units	16
Max Varying Components	64
Max Geometry Varying Components	64
Max Vertex Varying Components	32
Max Geometry Uniform Components	4096
Max Geometry Output Vertices	256
Max Geometry Total Output Components	1024

Fragment Shader:

Max Uniform Fragment Components	4096

Vertex Program:

Max Local Parameters	256
Max Environment Parameters	300
Max Program Matrices	8
Max Program Matrix Stack Depth	2
Max Vertex Attributes	16
Max Instructions	1024
Max Native Instructions	1024
Max Temporaries	31
Max Native Temporaries	31
Max Parameters	512
Max Native Parameters	400
Max Attributes	16
Max Native Attributes	16
Max Address Registers	1
Max Native Address Registers	1

Fragment Program:

Max Local Parameters	256
Max Environment Parameters	256
Max Texture Coordinates	8
Max Texture Image Units	16
Max Instructions	1447
Max Native Instructions	1447
Max Temporaries	256
Max Native Temporaries	256
Max Parameters	512
Max Native Parameters	32
Max Attributes	13
Max Native Attributes	13

Max Address Registers	0
Max Native Address Registers	0
Max ALU Instructions	1447
Max Native ALU Instructions	1447
Max Texture Instructions	1447
Max Native Texture Instructions	1447
Max Texture Indirections	128
Max Native Texture Indirections	128

Navigation

OpenGL Extensions:

Total / Supported Extensions	1073 / 188
GL_3DFX_multisample	Not Supported
GL_3DFX_tbuffer	Not Supported
GL_3DFX_texture_compression_FXT1	Supported
GL_3DL_direct_texture_access2	Not Supported
GL_3Dlabs_multisample_transparency_id	Not Supported
GL_3Dlabs_multisample_transparency_range	Not Supported
GL_AMD_blend_minmax_factor	Not Supported
GL_AMD_compressed_3DC_texture	Not Supported
GL_AMD_compressed_ATC_texture	Not Supported
GL_AMD_conservative_depth	Not Supported
GL_AMD_debug_output	Not Supported
GL_AMD_depth_clamp_separate	Not Supported
GL_AMD_draw_buffers_blend	Not Supported
GL_AMD_framebuffer_sample_positions	Not Supported
GL_AMD_gcn_shader	Not Supported
GL_AMD_gpu_shader_half_float	Not Supported
GL_AMD_gpu_shader_half_float_fetch	Not Supported
GL_AMD_gpu_shader_half_float2	Not Supported
GL_AMD_gpu_shader_int16	Not Supported
GL_AMD_gpu_shader_int64	Not Supported
GL_AMD_interleaved_elements	Not Supported
GL_AMD_multi_draw_indirect	Not Supported
GL_AMD_name_gen_delete	Not Supported
GL_AMD_occlusion_query_event	Not Supported
GL_AMD_performance_monitor	Not Supported
GL_AMD_pinned_memory	Not Supported
GL_AMD_program_binary_Z400	Not Supported
GL_AMD_query_buffer_object	Not Supported
GL_AMD_sample_positions	Not Supported
GL_AMD_seamless_cubemap_per_texture	Not Supported
GL_AMD_shader_atomic_counter_ops	Not Supported
GL_AMD_shader_stencil_export	Not Supported
GL_AMD_shader_stencil_value_export	Not Supported
GL_AMD_shader_trace	Not Supported
GL_AMD_shader_trinary_minmax	Not Supported
GL_AMD_sparse_texture	Not Supported
GL_AMD_sparse_texture_pool	Not Supported
GL_AMD_stencil_operation_extended	Not Supported
GL_AMD_texture_compression_dxt6	Not Supported
GL_AMD_texture_compression_dxt7	Not Supported
GL_AMD_texture_cube_map_array	Not Supported
GL_AMD_texture_texture4	Not Supported
GL_AMD_texture_tile_pool	Not Supported
GL_AMD_transform_feedback3_lines_triangles	Not Supported

Navigation

GL_AMD_transform_feedback4	Not Supported
GL_AMD_vertex_shader_layer	Not Supported
GL_AMD_vertex_shader_tessellator	Not Supported
GL_AMD_vertex_shader_viewport_index	Not Supported
GL_AMDX_debug_output	Not Supported
GL_AMDX_name_gen_delete	Not Supported
GL_AMDX_random_access_target	Not Supported
GL_AMDX_vertex_shader_tessellator	Not Supported
GL_ANDROID_extension_pack_es31a	Not Supported
GL_ANGLE_depth_texture	Not Supported
GL_ANGLE_framebuffer_blit	Not Supported
GL_ANGLE_framebuffer_multisample	Not Supported
GL_ANGLE_instanced_arrays	Not Supported
GL_ANGLE_pack_reverse_row_order	Not Supported
GL_ANGLE_program_binary	Not Supported
GL_ANGLE_texture_compression_dxt1	Not Supported
GL_ANGLE_texture_compression_dxt3	Not Supported
GL_ANGLE_texture_compression_dxt5	Not Supported
GL_ANGLE_texture_usage	Not Supported
GL_ANGLE_translated_shader_source	Not Supported
GL_APPLE_aux_depth_stencil	Not Supported
GL_APPLE_client_storage	Not Supported
GL_APPLE_copy_texture_levels	Not Supported
GL_APPLE_element_array	Not Supported
GL_APPLE_fence	Not Supported
GL_APPLE_float_pixels	Not Supported
GL_APPLE_flush_buffer_range	Not Supported
GL_APPLE_flush_render	Not Supported
GL_APPLE_framebuffer_multisample	Not Supported
GL_APPLE_object_purgeable	Not Supported
GL_APPLE_packed_pixel	Not Supported
GL_APPLE_packed_pixels	Not Supported
GL_APPLE_pixel_buffer	Not Supported
GL_APPLE_rgb_422	Not Supported
GL_APPLE_row_bytes	Not Supported
GL_APPLE_specular_vector	Not Supported
GL_APPLE_sync	Not Supported
GL_APPLE_texture_2D_limited_npot	Not Supported
GL_APPLE_texture_format_BGRA8888	Not Supported
GL_APPLE_texture_max_level	Not Supported
GL_APPLE_texture_range	Not Supported
GL_APPLE_transform_hint	Not Supported
GL_APPLE_vertex_array_object	Not Supported
GL_APPLE_vertex_array_range	Not Supported
GL_APPLE_vertex_point_size	Not Supported
GL_APPLE_vertex_program_evaluators	Not Supported
GL_APPLE_ycbcr_422	Not Supported
GL_ARB_arrays_of_arrays	Supported
GL_ARB_base_instance	Supported
GL_ARB_bindless_texture	Not Supported
GL_ARB_blend_func_extended	Supported
GL_ARB_buffer_storage	Supported
GL_ARB_cl_event	Not Supported
GL_ARB_clear_buffer_object	Not Supported
GL_ARB_clear_texture	Not Supported

GL_ARB_clip_control	Not Supported
GL_ARB_color_buffer_float	Supported
GL_ARB_compatibility	Supported
GL_ARB_compressed_texture_pixel_storage	Supported
GL_ARB_compute_shader	Not Supported
GL_ARB_compute_variable_group_size	Not Supported
GL_ARB_conditional_render_inverted	Not Supported
GL_ARB_conservative_depth	Supported
GL_ARB_context_flush_control	Not Supported
GL_ARB_copy_buffer	Supported
GL_ARB_copy_image	Not Supported
GL_ARB_cull_distance	Not Supported
GL_ARB_debug_group	Not Supported
GL_ARB_debug_label	Not Supported
GL_ARB_debug_output	Supported
GL_ARB_debug_output2	Not Supported
GL_ARB_depth_buffer_float	Supported
GL_ARB_depth_clamp	Supported
GL_ARB_depth_texture	Supported
GL_ARB_derivative_control	Not Supported
GL_ARB_direct_state_access	Not Supported
GL_ARB_draw_buffers	Supported
GL_ARB_draw_buffers_blend	Supported
GL_ARB_draw_elements_base_vertex	Supported
GL_ARB_draw_indirect	Supported
GL_ARB_draw_instanced	Supported
GL_ARB_enhanced_layouts	Not Supported
GL_ARB_ES2_compatibility	Supported
GL_ARB_ES3_1_compatibility	Not Supported
GL_ARB_ES3_2_compatibility	Not Supported
GL_ARB_ES3_compatibility	Supported
GL_ARB_explicit_attrib_location	Supported
GL_ARB_explicit_uniform_location	Not Supported
GL_ARB_fragment_coord_conventions	Supported
GL_ARB_fragment_layer_viewport	Not Supported
GL_ARB_fragment_program	Supported
GL_ARB_fragment_program_shadow	Supported
GL_ARB_fragment_shader	Supported
GL_ARB_fragment_shader_interlock	Not Supported
GL_ARB_framebuffer_no_attachments	Supported
GL_ARB_framebuffer_object	Supported
GL_ARB_framebuffer_sRGB	Supported
GL_ARB_geometry_shader4	Supported
GL_ARB_get_program_binary	Supported
GL_ARB_get_texture_sub_image	Not Supported
GL_ARB_gl_spirv	Not Supported
GL_ARB_gpu_shader_fp64	Supported
GL_ARB_gpu_shader_int64	Not Supported
GL_ARB_gpu_shader5	Supported
GL_ARB_half_float_pixel	Supported
GL_ARB_half_float_vertex	Supported
GL_ARB_imaging	Not Supported
GL_ARB_indirect_parameters	Not Supported
GL_ARB_instanced_arrays	Supported
GL_ARB_internalformat_query	Supported

Navigation

Navigation

GL_ARB_internalformat_query2	Supported
GL_ARB_invalidate_subdata	Not Supported
GL_ARB_make_current_read	Not Supported
GL_ARB_map_buffer_alignment	Supported
GL_ARB_map_buffer_range	Supported
GL_ARB_matrix_palette	Not Supported
GL_ARB_multi_bind	Not Supported
GL_ARB_multi_draw_indirect	Supported
GL_ARB_multisample	Supported
GL_ARB_multitexture	Supported
GL_ARB_occlusion_query	Supported
GL_ARB_occlusion_query2	Supported
GL_ARB_parallel_shader_compile	Not Supported
GL_ARB_pipeline_statistics_query	Not Supported
GL_ARB_pixel_buffer_object	Supported
GL_ARB_point_parameters	Supported
GL_ARB_point_sprite	Supported
GL_ARB_polygon_offset_clamp	Not Supported
GL_ARB_post_depth_coverage	Not Supported
GL_ARB_program_interface_query	Supported
GL_ARB_provoking_vertex	Supported
GL_ARB_query_buffer_object	Not Supported
GL_ARB_robust_buffer_access_behavior	Not Supported
GL_ARB_robustness	Supported
GL_ARB_robustness_isolation	Not Supported
GL_ARB_sample_locations	Not Supported
GL_ARB_sample_shading	Supported
GL_ARB_sampler_objects	Supported
GL_ARB_seamless_cube_map	Supported
GL_ARB_seamless_cubemap_per_texture	Not Supported
GL_ARB_separate_shader_objects	Supported
GL_ARB_shader_atomic_counter_ops	Not Supported
GL_ARB_shader_atomic_counters	Supported
GL_ARB_shader_ballot	Not Supported
GL_ARB_shader_bit_encoding	Supported
GL_ARB_shader_clock	Not Supported
GL_ARB_shader_draw_parameters	Not Supported
GL_ARB_shader_group_vote	Not Supported
GL_ARB_shader_image_load_store	Not Supported
GL_ARB_shader_image_size	Not Supported
GL_ARB_shader_objects	Supported
GL_ARB_shader_precision	Supported
GL_ARB_shader_stencil_export	Not Supported
GL_ARB_shader_storage_buffer_object	Not Supported
GL_ARB_shader_subroutine	Supported
GL_ARB_shader_texture_image_samples	Not Supported
GL_ARB_shader_texture_lod	Not Supported
GL_ARB_shader_viewport_layer_array	Not Supported
GL_ARB_shading_language_100	Supported
GL_ARB_shading_language_120	Not Supported
GL_ARB_shading_language_420pack	Supported
GL_ARB_shading_language_include	Not Supported
GL_ARB_shading_language_packing	Supported
GL_ARB_shadow	Supported
GL_ARB_shadow_ambient	Not Supported

GL_ARB_sparse_buffer	Not Supported
GL_ARB_sparse_texture	Not Supported
GL_ARB_sparse_texture_clamp	Not Supported
GL_ARB_sparse_texture2	Not Supported
GL_ARB_spirv_extensions	Not Supported
GL_ARB_stencil_texturing	Supported
GL_ARB_swap_buffers	Not Supported
GL_ARB_sync	Supported
GL_ARB_tessellation_shader	Supported
GL_ARB_texture_barrier	Not Supported
GL_ARB_texture_border_clamp	Supported
GL_ARB_texture_buffer_object	Not Supported
GL_ARB_texture_buffer_object_rgb32	Supported
GL_ARB_texture_buffer_range	Supported
GL_ARB_texture_compression	Supported
GL_ARB_texture_compression_bptc	Supported
GL_ARB_texture_compression_rgtc	Supported
GL_ARB_texture_compression_rtgc	Not Supported
GL_ARB_texture_cube_map	Supported
GL_ARB_texture_cube_map_array	Supported
GL_ARB_texture_env_add	Supported
GL_ARB_texture_env_combine	Supported
GL_ARB_texture_env_crossbar	Supported
GL_ARB_texture_env_dot3	Supported
GL_ARB_texture_filter_anisotropic	Not Supported
GL_ARB_texture_filter_minmax	Not Supported
GL_ARB_texture_float	Supported
GL_ARB_texture_gather	Supported
GL_ARB_texture_mirror_clamp_to_edge	Not Supported
GL_ARB_texture_mirrored_repeat	Not Supported
GL_ARB_texture_multisample	Supported
GL_ARB_texture_non_power_of_two	Supported
GL_ARB_texture_query_levels	Not Supported
GL_ARB_texture_query_lod	Supported
GL_ARB_texture_rectangle	Supported
GL_ARB_texture_rg	Supported
GL_ARB_texture_rgb10_a2ui	Supported
GL_ARB_texture_snorm	Not Supported
GL_ARB_texture_stencil8	Not Supported
GL_ARB_texture_storage	Supported
GL_ARB_texture_storage_multisample	Supported
GL_ARB_texture_swizzle	Supported
GL_ARB_texture_view	Not Supported
GL_ARB_timer_query	Supported
GL_ARB_transform_feedback_instanced	Supported
GL_ARB_transform_feedback_overflow_query	Not Supported
GL_ARB_transform_feedback2	Supported
GL_ARB_transform_feedback3	Supported
GL_ARB_transpose_matrix	Supported
GL_ARB_uber_buffers	Not Supported
GL_ARB_uber_mem_image	Not Supported
GL_ARB_uber_vertex_array	Not Supported
GL_ARB_uniform_buffer_object	Supported
GL_ARB_vertex_array_bgra	Supported
GL_ARB_vertex_array_object	Supported

Navigation

GL_ARB_vertex_attrib_64bit	Supported
GL_ARB_vertex_attrib_binding	Supported
GL_ARB_vertex_blend	Not Supported
GL_ARB_vertex_buffer_object	Supported
GL_ARB_vertex_program	Supported
GL_ARB_vertex_shader	Supported
GL_ARB_vertex_type_10f_11f_11f_rev	Not Supported
GL_ARB_vertex_type_2_10_10_10_rev	Supported
GL_ARB_viewport_array	Supported
GL_ARB_window_pos	Supported
GL_ARM_mali_program_binary	Not Supported
GL_ARM_mali_shader_binary	Not Supported
GL_ARM_rgba8	Not Supported
GL_ARM_shader_framebuffer_fetch	Not Supported
GL_ARM_shader_framebuffer_fetch_depth_stencil	Not Supported
GL_ATI_array_rev_comps_in_4_bytes	Not Supported
GL_ATI_blend_equation_separate	Not Supported
GL_ATI_blend_weighted_minmax	Not Supported
GL_ATI_draw_buffers	Not Supported
GL_ATI_element_array	Not Supported
GL_ATI_envmap_bumpmap	Not Supported
GL_ATI_fragment_shader	Not Supported
GL_ATI_lock_texture	Not Supported
GL_ATI_map_object_buffer	Not Supported
GL_ATI_meminfo	Not Supported
GL_ATI_pixel_format_float	Not Supported
GL_ATI_pn_triangles	Not Supported
GL_ATI_point_cull_mode	Not Supported
GL_ATI_separate_stencil	Supported
GL_ATI_shader_texture_lod	Not Supported
GL_ATI_text_fragment_shader	Not Supported
GL_ATI_texture_compression_3dc	Not Supported
GL_ATI_texture_env_combine3	Not Supported
GL_ATI_texture_float	Not Supported
GL_ATI_texture_mirror_once	Not Supported
GL_ATI_vertex_array_object	Not Supported
GL_ATI_vertex_attrib_array_object	Not Supported
GL_ATI_vertex_blend	Not Supported
GL_ATI_vertex_shader	Not Supported
GL_ATI_vertex_streams	Not Supported
GL_ATIX_pn_triangles	Not Supported
GL_ATIX_texture_env_combine3	Not Supported
GL_ATIX_texture_env_route	Not Supported
GL_ATIX_vertex_shader_output_point_size	Not Supported
GL_Autodesk_facet_normal	Not Supported
GL_Autodesk_valid_back_buffer_hint	Not Supported
GL_CR_bounding_box	Not Supported
GL_CR_cursor_position	Not Supported
GL_CR_head_spu_name	Not Supported
GL_CR_performance_info	Not Supported
GL_CR_print_string	Not Supported
GL_CR_readback_barrier_size	Not Supported
GL_CR_saveframe	Not Supported
GL_CR_server_id_sharing	Not Supported
GL_CR_server_matrix	Not Supported

Navigation

GL_CR_state_parameter	Not Supported
GL_CR_synchronization	Not Supported
GL_CR_tile_info	Not Supported
GL_CR_tilesort_info	Not Supported
GL_CR_window_size	Not Supported
GL_DIMD_YUV	Not Supported
GL_DMP_shader_binary	Not Supported
GL_EXT_422_pixels	Not Supported
GL_EXT_abgr	Supported
GL_EXT_bgra	Supported
GL_EXT_bindable_uniform	Not Supported
GL_EXT_blend_color	Supported
GL_EXT_blend_equation_separate	Supported
GL_EXT_blend_func_separate	Supported
GL_EXT_blend_logic_op	Not Supported
GL_EXT_blend_minmax	Supported
GL_EXT_blend_subtract	Supported
GL_EXT_Cg_shader	Not Supported
GL_EXT_clip_control	Not Supported
GL_EXT_clip_volume_hint	Supported
GL_EXT_cmyka	Not Supported
GL_EXT_color_buffer_float	Not Supported
GL_EXT_color_buffer_half_float	Not Supported
GL_EXT_color_matrix	Not Supported
GL_EXT_color_subtable	Not Supported
GL_EXT_color_table	Not Supported
GL_EXT_compiled_vertex_array	Supported
GL_EXT_convolution	Not Supported
GL_EXT_convolution_border_modes	Not Supported
GL_EXT_coordinate_frame	Not Supported
GL_EXT_copy_buffer	Not Supported
GL_EXT_copy_image	Not Supported
GL_EXT_copy_texture	Not Supported
GL_EXT_cull_vertex	Not Supported
GL_EXT_debug_label	Not Supported
GL_EXT_debug_marker	Not Supported
GL_EXT_depth_bounds_test	Not Supported
GL_EXT_depth_buffer_float	Not Supported
GL_EXT_direct_state_access	Not Supported
GL_EXT_discard_framebuffer	Not Supported
GL_EXT_disjoint_timer_query	Not Supported
GL_EXT_draw_buffers	Not Supported
GL_EXT_draw_buffers_indexed	Not Supported
GL_EXT_draw_buffers2	Supported
GL_EXT_draw_indirect	Not Supported
GL_EXT_draw_instanced	Not Supported
GL_EXT_draw_range_elements	Supported
GL_EXT_fog_coord	Supported
GL_EXT_fog_function	Not Supported
GL_EXT_fog_offset	Not Supported
GL_EXT_frag_depth	Not Supported
GL_EXT_fragment_lighting	Not Supported
GL_EXT_framebuffer_blit	Supported
GL_EXT_framebuffer_multisample	Supported
GL_EXT_framebuffer_multisample_blit_scaled	Not Supported

Navigation

GL_EXT_framebuffer_object	Supported
GL_EXT_framebuffer_sRGB	Not Supported
GL_EXT_generate_mipmap	Not Supported
GL_EXT_geometry_point_size	Not Supported
GL_EXT_geometry_shader	Not Supported
GL_EXT_geometry_shader4	Supported
GL_EXT_glx_stereo_tree	Not Supported
GL_EXT_gpu_program_parameters	Supported
GL_EXT_gpu_shader_fp64	Not Supported
GL_EXT_gpu_shader4	Supported
GL_EXT_gpu_shader5	Not Supported
GL_EXT_histogram	Not Supported
GL_EXT_import_sync_object	Not Supported
GL_EXT_index_array_formats	Not Supported
GL_EXT_index_func	Not Supported
GL_EXT_index_material	Not Supported
GL_EXT_index_texture	Not Supported
GL_EXT_instanced_arrays	Not Supported
GL_EXT_interlace	Not Supported
GL_EXT_light_texture	Not Supported
GL_EXT_map_buffer_range	Not Supported
GL_EXT_memory_object	Not Supported
GL_EXT_memory_object_win32	Not Supported
GL_EXT_misc_attribute	Not Supported
GL_EXT_multi_draw_arrays	Supported
GL_EXT_multisample	Not Supported
GL_EXT_multisampled_render_to_texture	Not Supported
GL_EXT_multiview_draw_buffers	Not Supported
GL_EXT_occlusion_query_boolean	Not Supported
GL_EXT_packed_depth_stencil	Supported
GL_EXT_packed_float	Supported
GL_EXT_packed_pixels	Supported
GL_EXT_packed_pixels_12	Not Supported
GL_EXT_paletted_texture	Not Supported
GL_EXT_pixel_buffer_object	Not Supported
GL_EXT_pixel_format	Not Supported
GL_EXT_pixel_texture	Not Supported
GL_EXT_pixel_transform	Not Supported
GL_EXT_pixel_transform_color_table	Not Supported
GL_EXT_point_parameters	Not Supported
GL_EXT_polygon_offset	Not Supported
GL_EXT_polygon_offset_clamp	Not Supported
GL_EXT_post_depth_coverage	Not Supported
GL_EXT_primitive_bounding_box	Not Supported
GL_EXT_provoking_vertex	Not Supported
GL_EXT_pvrtc_sRGB	Not Supported
GL_EXT_raster_multisample	Not Supported
GL_EXT_read_format_bgra	Not Supported
GL_EXT_rescale_normal	Supported
GL_EXT_robustness	Not Supported
GL_EXT_scene_marker	Not Supported
GL_EXT_secondary_color	Supported
GL_EXT_semaphore	Not Supported
GL_EXT_semaphore_win32	Not Supported
GL_EXT_separate_shader_objects	Not Supported

Navigation

GL_EXT_separate_specular_color	Supported
GL_EXT_shader_atomic_counters	Not Supported
GL_EXT_shader_framebuffer_fetch	Not Supported
GL_EXT_shader_image_load_formatted	Not Supported
GL_EXT_shader_image_load_store	Not Supported
GL_EXT_shader_implicit_conversions	Not Supported
GL_EXT_shader_integer_mix	Supported
GL_EXT_shader_io_blocks	Not Supported
GL_EXT_shader_pixel_local_storage	Not Supported
GL_EXT_shader_subroutine	Not Supported
GL_EXT_shader_texture_lod	Not Supported
GL_EXT_shadow_funcs	Supported
GL_EXT_shadow_samplers	Not Supported
GL_EXT_shared_texture_palette	Not Supported
GL_EXT_sparse_texture2	Not Supported
GL_EXT_sRGB	Not Supported
GL_EXT_sRGB_write_control	Not Supported
GL_EXT_static_vertex_array	Not Supported
GL_EXT_stencil_clear_tag	Not Supported
GL_EXT_stencil_two_side	Supported
GL_EXT_stencil_wrap	Supported
GL_EXT_subtexture	Not Supported
GL_EXT_swap_control	Not Supported
GL_EXT_tessellation_point_size	Not Supported
GL_EXT_tessellation_shader	Not Supported
GL_EXT_texgen_reflection	Not Supported
GL_EXT_texture	Not Supported
GL_EXT_texture_array	Supported
GL_EXT_texture_border_clamp	Not Supported
GL_EXT_texture_buffer	Supported
GL_EXT_texture_buffer_object	Not Supported
GL_EXT_texture_buffer_object_rgb32	Not Supported
GL_EXT_texture_color_table	Not Supported
GL_EXT_texture_compression_bptc	Not Supported
GL_EXT_texture_compression_dxt1	Not Supported
GL_EXT_texture_compression_latc	Not Supported
GL_EXT_texture_compression_rgtc	Not Supported
GL_EXT_texture_compression_s3tc	Supported
GL_EXT_texture_cube_map	Not Supported
GL_EXT_texture_cube_map_array	Not Supported
GL_EXT_texture_edge_clamp	Supported
GL_EXT_texture_env	Not Supported
GL_EXT_texture_env_add	Supported
GL_EXT_texture_env_combine	Supported
GL_EXT_texture_env_dot3	Not Supported
GL_EXT_texture_filter_anisotropic	Supported
GL_EXT_texture_filter_minmax	Not Supported
GL_EXT_texture_format_BGRA8888	Not Supported
GL_EXT_texture_integer	Supported
GL_EXT_texture_lod	Not Supported
GL_EXT_texture_lod_bias	Supported
GL_EXT_texture_mirror_clamp	Not Supported
GL_EXT_texture_object	Not Supported
GL_EXT_texture_perturb_normal	Not Supported
GL_EXT_texture_rectangle	Supported

Navigation

GL_EXT_texture_rg	Not Supported
GL_EXT_texture_shared_exponent	Supported
GL_EXT_texture_snorm	Supported
GL_EXT_texture_sRGB	Supported
GL_EXT_texture_sRGB_decode	Supported
GL_EXT_texture_sRGB_R8	Not Supported
GL_EXT_texture_storage	Supported
GL_EXT_texture_swizzle	Supported
GL_EXT_texture_type_2_10_10_10_REV	Not Supported
GL_EXT_texture_view	Not Supported
GL_EXT_texture3D	Supported
GL_EXT_texture4D	Not Supported
GL_EXT_timer_query	Not Supported
GL_EXT_transform_feedback	Supported
GL_EXT_transform_feedback2	Not Supported
GL_EXT_transform_feedback3	Not Supported
GL_EXT_unpack_subimage	Not Supported
GL_EXT_vertex_array	Not Supported
GL_EXT_vertex_array_bgra	Not Supported
GL_EXT_vertex_array_set	Not Supported
GL_EXT_vertex_array_setXXX	Not Supported
GL_EXT_vertex_attrib_64bit	Not Supported
GL_EXT_vertex_shader	Not Supported
GL_EXT_vertex_weighting	Not Supported
GL_EXT_win32_keyed_mutex	Not Supported
GL_EXT_window_rectangles	Not Supported
GL_EXT_x11_sync_object	Not Supported
GL_EXTX_framebuffer_mixed_formats	Not Supported
GL_EXTX_packed_depth_stencil	Not Supported
GL_FGL_lock_texture	Not Supported
GL_FJ_shader_binary_GCCSO	Not Supported
GL_GL2_geometry_shader	Not Supported
GL_GREMEDY_frame_terminator	Not Supported
GL_GREMEDY_string_marker	Not Supported
GL_HP_convolution_border_modes	Not Supported
GL_HP_image_transform	Not Supported
GL_HP_occlusion_test	Not Supported
GL_HP_texture_lighting	Not Supported
GL_I3D_argb	Not Supported
GL_I3D_color_clamp	Not Supported
GL_I3D_interlace_read	Not Supported
GL_IBM_clip_check	Not Supported
GL_IBM_cull_vertex	Not Supported
GL_IBM_load_named_matrix	Not Supported
GL_IBM_multi_draw_arrays	Not Supported
GL_IBM_multimode_draw_arrays	Not Supported
GL_IBM_occlusion_cull	Not Supported
GL_IBM_pixel_filter_hint	Not Supported
GL_IBM_rasterpos_clip	Not Supported
GL_IBM_rescale_normal	Not Supported
GL_IBM_static_data	Not Supported
GL_IBM_texture_clamp_nodraw	Not Supported
GL_IBM_texture_mirrored_repeat	Supported
GL_IBM_vertex_array_lists	Not Supported
GL_IBM_YCbCr	Not Supported

Navigation

GL_IMG_multisampled_render_to_texture	Not Supported
GL_IMG_program_binary	Not Supported
GL_IMG_read_format	Not Supported
GL_IMG_sgx_binary	Not Supported
GL_IMG_shader_binary	Not Supported
GL_IMG_texture_compression_pvrtc	Not Supported
GL_IMG_texture_compression_pvrtc2	Not Supported
GL_IMG_texture_env_enhanced_fixed_function	Not Supported
GL_IMG_texture_format_BGRA8888	Not Supported
GL_IMG_user_clip_plane	Not Supported
GL_IMG_vertex_program	Not Supported
GL_INGR_blend_func_separate	Not Supported
GL_INGR_color_clamp	Not Supported
GL_INGR_interlace_read	Not Supported
GL_INGR_multiple_palette	Not Supported
GL_INTEL_coarse_fragment_shader	Not Supported
GL_INTEL_compute_shader_lane_shift	Not Supported
GL_INTEL_conservative_rasterization	Not Supported
GL_INTEL_fragment_shader_ordering	Not Supported
GL_INTEL_fragment_shader_span_sharing	Not Supported
GL_INTEL_framebuffer_CMAA	Not Supported
GL_INTEL_image_serialize	Not Supported
GL_INTEL_map_texture	Supported
GL_INTEL_multi_rate_fragment_shader	Not Supported
GL_INTEL_parallel_arrays	Not Supported
GL_INTEL_performance_queries	Supported
GL_INTEL_performance_query	Supported
GL_INTEL_texture_scissor	Not Supported
GL_KHR_blend_equation_advanced	Supported
GL_KHR_blend_equation_advanced_coherent	Not Supported
GL_KHR_context_flush_control	Not Supported
GL_KHR_debug	Supported
GL_KHR_no_error	Not Supported
GL_KHR_parallel_shader_compile	Not Supported
GL_KHR_robust_buffer_access_behavior	Not Supported
GL_KHR_robustness	Not Supported
GL_KHR_texture_compression_astc_hdr	Not Supported
GL_KHR_texture_compression_astc_ldr	Not Supported
GL_KHR_vulkan_glsl	Not Supported
GL_KTX_buffer_region	Not Supported
GL_MESA_pack_invert	Not Supported
GL_MESA_program_debug	Not Supported
GL_MESA_resize_buffers	Not Supported
GL_MESA_texture_array	Not Supported
GL_MESA_texture_signed_rgba	Not Supported
GL_MESA_window_pos	Not Supported
GL_MESA_ycbcr_texture	Not Supported
GL_MESAX_texture_float	Not Supported
GL_MESAX_texture_stack	Not Supported
GL_MTX_fragment_shader	Not Supported
GL_MTX_precision_dpi	Not Supported
GL_NV_3dvision_settings	Not Supported
GL_NV_alpha_test	Not Supported
GL_NV_alpha_to_coverage_dither_control	Not Supported
GL_NV_bgr	Not Supported

Navigation

GL_NV_bindless_multi_draw_indirect	Not Supported
GL_NV_bindless_multi_draw_indirect_count	Not Supported
GL_NV_bindless_texture	Not Supported
GL_NV_blend_equation_advanced	Not Supported
GL_NV_blend_equation_advanced_coherent	Not Supported
GL_NV_blend_minmax	Not Supported
GL_NV_blend_minmax_factor	Not Supported
GL_NV_blend_square	Supported
GL_NV_centroid_sample	Not Supported
GL_NV_clip_space_w_scaling	Not Supported
GL_NV_command_list	Not Supported
GL_NV_complex_primitives	Not Supported
GL_NV_compute_program5	Not Supported
GL_NV_compute_shader_derivatives	Not Supported
GL_NV_conditional_render	Supported
GL_NV_conservative_raster	Not Supported
GL_NV_conservative_raster_dilate	Not Supported
GL_NV_conservative_raster_pre_snap	Not Supported
GL_NV_conservative_raster_pre_snap_triangles	Not Supported
GL_NV_conservative_raster_underestimation	Not Supported
GL_NV_copy_buffer	Not Supported
GL_NV_copy_depth_to_color	Not Supported
GL_NV_copy_image	Not Supported
GL_NV_coverage_sample	Not Supported
GL_NV_deep_texture3D	Not Supported
GL_NV_depth_buffer_float	Not Supported
GL_NV_depth_clamp	Not Supported
GL_NV_depth_nonlinear	Not Supported
GL_NV_depth_range_unclamped	Not Supported
GL_NV_draw_buffers	Not Supported
GL_NV_draw_instanced	Not Supported
GL_NV_draw_texture	Not Supported
GL_NV_draw_vulkan_image	Not Supported
GL_NV_EGL_stream_consumer_external	Not Supported
GL_NV_ES1_1_compatibility	Not Supported
GL_NV_ES3_1_compatibility	Not Supported
GL_NV_evaluators	Not Supported
GL_NV_explicit_attrib_location	Not Supported
GL_NV_explicit_multisample	Not Supported
GL_NV_fbo_color_attachments	Not Supported
GL_NV_feature_query	Not Supported
GL_NV_fence	Not Supported
GL_NV_fill_rectangle	Not Supported
GL_NV_float_buffer	Not Supported
GL_NV_fog_distance	Not Supported
GL_NV_fragdepth	Not Supported
GL_NV_fragment_coverage_to_color	Not Supported
GL_NV_fragment_program	Not Supported
GL_NV_fragment_program_option	Not Supported
GL_NV_fragment_program2	Not Supported
GL_NV_fragment_program4	Not Supported
GL_NV_fragment_shader_barycentric	Not Supported
GL_NV_fragment_shader_interlock	Not Supported
GL_NV_framebuffer_blit	Not Supported
GL_NV_framebuffer_mixed_samples	Not Supported

Navigation

Navigation

GL_NV_framebuffer_multisample	Not Supported
GL_NV_framebuffer_multisample_coverage	Not Supported
GL_NV_framebuffer_multisample_ex	Not Supported
GL_NV_generate_mipmap_sRGB	Not Supported
GL_NV_geometry_program4	Not Supported
GL_NV_geometry_shader_passthrough	Not Supported
GL_NV_geometry_shader4	Not Supported
GL_NV_gpu_program_fp64	Not Supported
GL_NV_gpu_program4	Not Supported
GL_NV_gpu_program4_1	Not Supported
GL_NV_gpu_program5	Not Supported
GL_NV_gpu_program5_mem_extended	Not Supported
GL_NV_gpu_shader5	Not Supported
GL_NV_half_float	Not Supported
GL_NV_instanced_arrays	Not Supported
GL_NV_internalformat_sample_query	Not Supported
GL_NV_light_max_exponent	Not Supported
GL_NV_memory_attachment	Not Supported
GL_NV_mesh_shader	Not Supported
GL_NV_multisample_coverage	Not Supported
GL_NV_multisample_filter_hint	Not Supported
GL_NV_non_square_matrices	Not Supported
GL_NV_occlusion_query	Not Supported
GL_NV_pack_subimage	Not Supported
GL_NV_packed_depth_stencil	Not Supported
GL_NV_packed_float	Not Supported
GL_NV_packed_float_linear	Not Supported
GL_NV_parameter_buffer_object	Not Supported
GL_NV_parameter_buffer_object2	Not Supported
GL_NV_path_rendering	Not Supported
GL_NV_path_rendering_shared_edge	Not Supported
GL_NV_pixel_buffer_object	Not Supported
GL_NV_pixel_data_range	Not Supported
GL_NV_platform_binary	Not Supported
GL_NV_point_sprite	Not Supported
GL_NV_present_video	Not Supported
GL_NV_primitive_restart	Supported
GL_NV_query_resource	Not Supported
GL_NV_query_resource_tag	Not Supported
GL_NV_read_buffer	Not Supported
GL_NV_read_buffer_front	Not Supported
GL_NV_read_depth	Not Supported
GL_NV_read_depth_stencil	Not Supported
GL_NV_read_stencil	Not Supported
GL_NV_register_combiners	Not Supported
GL_NV_register_combiners2	Not Supported
GL_NV_representative_fragment_test	Not Supported
GL_NV_robustness_video_memory_purge	Not Supported
GL_NV_sample_locations	Not Supported
GL_NV_sample_mask_override_coverage	Not Supported
GL_NV_scissor_exclusive	Not Supported
GL_NV_shader_atomic_counters	Not Supported
GL_NV_shader_atomic_float	Not Supported
GL_NV_shader_atomic_float64	Not Supported
GL_NV_shader_atomic_fp16_vector	Not Supported

Navigation

GL_NV_shader_atomic_int64	Not Supported
GL_NV_shader_buffer_load	Not Supported
GL_NV_shader_buffer_store	Not Supported
GL_NV_shader_storage_buffer_object	Not Supported
GL_NV_shader_texture_footprint	Not Supported
GL_NV_shader_thread_group	Not Supported
GL_NV_shader_thread_shuffle	Not Supported
GL_NV_shading_rate_image	Not Supported
GL_NV_shadow_samplers_array	Not Supported
GL_NV_shadow_samplers_cube	Not Supported
GL_NV_sRGB_formats	Not Supported
GL_NV_stereo_view_rendering	Not Supported
GL_NV_tessellation_program5	Not Supported
GL_NV_texgen_emboss	Not Supported
GL_NV_texgen_reflection	Supported
GL_NV_texture_array	Not Supported
GL_NV_texture_barrier	Not Supported
GL_NV_texture_border_clamp	Not Supported
GL_NV_texture_compression_latc	Not Supported
GL_NV_texture_compression_s3tc	Not Supported
GL_NV_texture_compression_s3tc_update	Not Supported
GL_NV_texture_compression_vtc	Not Supported
GL_NV_texture_env_combine4	Not Supported
GL_NV_texture_expand_normal	Not Supported
GL_NV_texture_lod_clamp	Not Supported
GL_NV_texture_multisample	Not Supported
GL_NV_texture_npot_2D_mipmap	Not Supported
GL_NV_texture_rectangle	Not Supported
GL_NV_texture_rectangle_compressed	Not Supported
GL_NV_texture_shader	Not Supported
GL_NV_texture_shader2	Not Supported
GL_NV_texture_shader3	Not Supported
GL_NV_timer_query	Not Supported
GL_NV_transform_feedback	Not Supported
GL_NV_transform_feedback2	Not Supported
GL_NV_uniform_buffer_unified_memory	Not Supported
GL_NV_vdpau_interop	Not Supported
GL_NV_vertex_array_range	Not Supported
GL_NV_vertex_array_range2	Not Supported
GL_NV_vertex_attrib_64bit	Not Supported
GL_NV_vertex_attrib_integer_64bit	Not Supported
GL_NV_vertex_buffer_unified_memory	Not Supported
GL_NV_vertex_program	Not Supported
GL_NV_vertex_program1_1	Not Supported
GL_NV_vertex_program2	Not Supported
GL_NV_vertex_program2_option	Not Supported
GL_NV_vertex_program3	Not Supported
GL_NV_vertex_program4	Not Supported
GL_NV_video_capture	Not Supported
GL_NV_viewport_array2	Not Supported
GL_NV_viewport_swizzle	Not Supported
GL_NVX_blend_equation_advanced_multi_draw_buffers	Not Supported
GL_NVX_conditional_render	Not Supported
GL_NVX_flush_hold	Not Supported
GL_NVX_gpu_memory_info	Not Supported

Navigation

GL_NVX_instanced_arrays	Not Supported
GL_NVX_multigpu_info	Not Supported
GL_NVX_nvenc_interop	Not Supported
GL_NVX_shader_thread_group	Not Supported
GL_NVX_shader_thread_shuffle	Not Supported
GL_NVX_shared_sync_object	Not Supported
GL_NVX_sysmem_buffer	Not Supported
GL_NVX_ycrcb	Not Supported
GL_OES_blend_equation_separate	Not Supported
GL_OES_blend_func_separate	Not Supported
GL_OES_blend_subtract	Not Supported
GL_OES_byte_coordinates	Not Supported
GL_OES_compressed_EAC_R11_signed_texture	Not Supported
GL_OES_compressed_EAC_R11_unsigned_texture	Not Supported
GL_OES_compressed_EAC_RG11_signed_texture	Not Supported
GL_OES_compressed_EAC_RG11_unsigned_texture	Not Supported
GL_OES_compressed_ETC1_RGB8_texture	Not Supported
GL_OES_compressed_ETC2_punchthroughA_RGBA8_texture	Not Supported
GL_OES_compressed_ETC2_punchthroughA_sRGB8_alpha_texture	Not Supported
GL_OES_compressed_ETC2_RGB8_texture	Not Supported
GL_OES_compressed_ETC2_RGBA8_texture	Not Supported
GL_OES_compressed_ETC2_sRGB8_alpha8_texture	Not Supported
GL_OES_compressed_ETC2_sRGB8_texture	Not Supported
GL_OES_compressed_paletted_texture	Not Supported
GL_OES_conditional_query	Not Supported
GL_OES_depth_texture	Not Supported
GL_OES_depth_texture_cube_map	Not Supported
GL_OES_depth24	Not Supported
GL_OES_depth32	Not Supported
GL_OES_draw_texture	Not Supported
GL_OES_EGL_image	Not Supported
GL_OES_EGL_image_external	Not Supported
GL_OES_EGL_sync	Not Supported
GL_OES_element_index_uint	Not Supported
GL_OES_extended_matrix_palette	Not Supported
GL_OES_fbo_render_mipmap	Not Supported
GL_OES_fixed_point	Not Supported
GL_OES_fragment_precision_high	Not Supported
GL_OES_framebuffer_object	Not Supported
GL_OES_get_program_binary	Not Supported
GL_OES_mapbuffer	Not Supported
GL_OES_matrix_get	Not Supported
GL_OES_matrix_palette	Not Supported
GL_OES_packed_depth_stencil	Not Supported
GL_OES_point_size_array	Not Supported
GL_OES_point_sprite	Not Supported
GL_OES_query_matrix	Not Supported
GL_OES_read_format	Not Supported
GL_OES_required_internalformat	Not Supported
GL_OES_rgb8_rgba8	Not Supported
GL_OES_sample_shading	Not Supported
GL_OES_sample_variables	Not Supported
GL_OES_shader_image_atomic	Not Supported
GL_OES_shader_multisample_interpolation	Not Supported
GL_OES_single_precision	Not Supported

GL_OES_standard_derivatives	Not Supported
GL_OES_stencil_wrap	Not Supported
GL_OES_stencil1	Not Supported
GL_OES_stencil4	Not Supported
GL_OES_stencil8	Not Supported
GL_OES_surfaceless_context	Not Supported
GL_OES_texture_3D	Not Supported
GL_OES_texture_compression_astc	Not Supported
GL_OES_texture_cube_map	Not Supported
GL_OES_texture_env_crossbar	Not Supported
GL_OES_texture_float	Not Supported
GL_OES_texture_float_linear	Not Supported
GL_OES_texture_half_float	Not Supported
GL_OES_texture_half_float_linear	Not Supported
GL_OES_texture_mirrored_repeat	Not Supported
GL_OES_texture_npot	Not Supported
GL_OES_texture_stencil8	Not Supported
GL_OES_texture_storage_multisample_2d_array	Not Supported
GL_OES_vertex_array_object	Not Supported
GL_OES_vertex_half_float	Not Supported
GL_OES_vertex_type_10_10_10_2	Not Supported
GL_OML_interlace	Not Supported
GL_OML_resample	Not Supported
GL_OML_subsample	Not Supported
GL_OVR_multiview	Not Supported
GL_OVR_multiview2	Not Supported
GL_PGI_misc_hints	Not Supported
GL_PGI_vertex_hints	Not Supported
GL_QCOM_alpha_test	Not Supported
GL_QCOM_binning_control	Not Supported
GL_QCOM_driver_control	Not Supported
GL_QCOM_extended_get	Not Supported
GL_QCOM_extended_get2	Not Supported
GL_QCOM_perfmon_global_mode	Not Supported
GL_QCOM_tiled_rendering	Not Supported
GL_QCOM_writeonly_rendering	Not Supported
GL_REND_screen_coordinates	Not Supported
GL_S3_performance_analyzer	Not Supported
GL_S3_s3tc	Not Supported
GL_S3_texture_float_linear	Not Supported
GL_S3_texture_half_float_linear	Not Supported
GL_SGI_color_matrix	Not Supported
GL_SGI_color_table	Not Supported
GL_SGI_compiled_vertex_array	Not Supported
GL_SGI_cull_vertex	Not Supported
GL_SGI_index_array_formats	Not Supported
GL_SGI_index_func	Not Supported
GL_SGI_index_material	Not Supported
GL_SGI_index_texture	Not Supported
GL_SGI_make_current_read	Not Supported
GL_SGI_texture_add_env	Not Supported
GL_SGI_texture_color_table	Not Supported
GL_SGI_texture_edge_clamp	Not Supported
GL_SGI_texture_lod	Not Supported
GL_SGIS_color_range	Not Supported

Navigation

GL_SGIS_detail_texture	Not Supported
GL_SGIS_fog_function	Not Supported
GL_SGIS_generate_mipmap	Supported
GL_SGIS_multisample	Not Supported
GL_SGIS_multitexture	Not Supported
GL_SGIS_pixel_texture	Not Supported
GL_SGIS_point_line_texgen	Not Supported
GL_SGIS_sharpen_texture	Not Supported
GL_SGIS_texture_border_clamp	Not Supported
GL_SGIS_texture_color_mask	Not Supported
GL_SGIS_texture_edge_clamp	Supported
GL_SGIS_texture_filter4	Not Supported
GL_SGIS_texture_lod	Supported
GL_SGIS_texture_select	Not Supported
GL_SGIS_texture4D	Not Supported
GL_SGIX_async	Not Supported
GL_SGIX_async_histogram	Not Supported
GL_SGIX_async_pixel	Not Supported
GL_SGIX_blend_alpha_minmax	Not Supported
GL_SGIX_clipmap	Not Supported
GL_SGIX_convolution_accuracy	Not Supported
GL_SGIX_depth_pass_instrument	Not Supported
GL_SGIX_depth_texture	Not Supported
GL_SGIX_flush_raster	Not Supported
GL_SGIX_fog_offset	Not Supported
GL_SGIX_fog_texture	Not Supported
GL_SGIX_fragment_specular_lighting	Not Supported
GL_SGIX_framezoom	Not Supported
GL_SGIX_instruments	Not Supported
GL_SGIX_interlace	Not Supported
GL_SGIX_ir_instrument1	Not Supported
GL_SGIX_list_priority	Not Supported
GL_SGIX_pbuffer	Not Supported
GL_SGIX_pixel_texture	Not Supported
GL_SGIX_pixel_texture_bits	Not Supported
GL_SGIX_reference_plane	Not Supported
GL_SGIX_resample	Not Supported
GL_SGIX_shadow	Not Supported
GL_SGIX_shadow_ambient	Not Supported
GL_SGIX_sprite	Not Supported
GL_SGIX_subsample	Not Supported
GL_SGIX_tag_sample_buffer	Not Supported
GL_SGIX_texture_add_env	Not Supported
GL_SGIX_texture_coordinate_clamp	Not Supported
GL_SGIX_texture_lod_bias	Not Supported
GL_SGIX_texture_multi_buffer	Not Supported
GL_SGIX_texture_range	Not Supported
GL_SGIX_texture_scale_bias	Not Supported
GL_SGIX_vertex_preclip	Not Supported
GL_SGIX_vertex_preclip_hint	Not Supported
GL_SGIX_ycrcb	Not Supported
GL_SGIX_ycrcb_subsample	Not Supported
GL_SUN_convolution_border_modes	Not Supported
GL_SUN_global_alpha	Not Supported
GL_SUN_mesh_array	Not Supported

Navigation

GL_SUN_multi_draw_arrays	Supported
GL_SUN_read_video_pixels	Not Supported
GL_SUN_slice_accum	Not Supported
GL_SUN_triangle_list	Not Supported
GL_SUN_vertex	Not Supported
GL_SUNX_constant_data	Not Supported
GL_VIV_shader_binary	Not Supported
GL_WGL_ARB_extensions_string	Not Supported
GL_WGL_EXT_extensions_string	Not Supported
GL_WGL_EXT_swap_control	Not Supported
GL_WIN_phong_shading	Not Supported
GL_WIN_specular_fog	Not Supported
GL_WIN_swap_hint	Supported
GLU_EXT_nurbs_tessellator	Not Supported
GLU_EXT_object_space_tess	Not Supported
GLU_SGI_filter4_parameters	Not Supported
GLX_AMD_gpu_association	Not Supported
GLX_ARB_create_context	Not Supported
GLX_ARB_create_context_no_error	Not Supported
GLX_ARB_create_context_profile	Not Supported
GLX_ARB_create_context_robustness	Not Supported
GLX_ARB_fbconfig_float	Not Supported
GLX_ARB_framebuffer_sRGB	Not Supported
GLX_ARB_get_proc_address	Not Supported
GLX_ARB_multisample	Not Supported
GLX_ARB_robustness_application_isolation	Not Supported
GLX_ARB_robustness_share_group_isolation	Not Supported
GLX_ARB_vertex_buffer_object	Not Supported
GLX_EXT_buffer_age	Not Supported
GLX_EXT_create_context_es_profile	Not Supported
GLX_EXT_create_context_es2_profile	Not Supported
GLX_EXT_fbconfig_packed_float	Not Supported
GLX_EXT_framebuffer_sRGB	Not Supported
GLX_EXT_import_context	Not Supported
GLX_EXT_scene_marker	Not Supported
GLX_EXT_swap_control	Not Supported
GLX_EXT_swap_control_tear	Not Supported
GLX_EXT_texture_from_pixmap	Not Supported
GLX_EXT_visual_info	Not Supported
GLX_EXT_visual_rating	Not Supported
GLX_INTEL_swap_event	Not Supported
GLX_MESA_agp_offset	Not Supported
GLX_MESA_copy_sub_buffer	Not Supported
GLX_MESA_multithread_makecurrent	Not Supported
GLX_MESA_pixmap_colormap	Not Supported
GLX_MESA_query_renderer	Not Supported
GLX_MESA_release_buffers	Not Supported
GLX_MESA_set_3dfx_mode	Not Supported
GLX_MESA_swap_control	Not Supported
GLX_NV_copy_image	Not Supported
GLX_NV_delay_before_swap	Not Supported
GLX_NV_float_buffer	Not Supported
GLX_NV_multisample_coverage	Not Supported
GLX_NV_present_video	Not Supported
GLX_NV_swap_group	Not Supported

Navigation

GLX_NV_video_capture	Not Supported
GLX_NV_video_out	Not Supported
GLX_NV_video_output	Not Supported
GLX_OML_interlace	Not Supported
GLX_OML_swap_method	Not Supported
GLX_OML_sync_control	Not Supported
GLX_SGI_cushion	Not Supported
GLX_SGI_make_current_read	Not Supported
GLX_SGI_swap_control	Not Supported
GLX_SGI_video_sync	Not Supported
GLX_SGIS_blended_overlay	Not Supported
GLX_SGIS_color_range	Not Supported
GLX_SGIS_multisample	Not Supported
GLX_SGIX_dm_buffer	Not Supported
GLX_SGIX_fbconfig	Not Supported
GLX_SGIX_hyperpipe	Not Supported
GLX_SGIX_pbuffer	Not Supported
GLX_SGIX_swap_barrier	Not Supported
GLX_SGIX_swap_group	Not Supported
GLX_SGIX_video_resize	Not Supported
GLX_SGIX_video_source	Not Supported
GLX_SGIX_visual_select_group	Not Supported
GLX_SUN_get_transparent_index	Not Supported
GLX_SUN_video_resize	Not Supported
WGL_3DFX_gamma_control	Not Supported
WGL_3DFX_multisample	Not Supported
WGL_3DL_stereo_control	Not Supported
WGL_AMD_gpu_association	Not Supported
WGL_AMDX_gpu_association	Not Supported
WGL_ARB_buffer_region	Supported
WGL_ARB_context_flush_control	Not Supported
WGL_ARB_create_context	Supported
WGL_ARB_create_context_no_error	Not Supported
WGL_ARB_create_context_profile	Supported
WGL_ARB_create_context_robustness	Supported
WGL_ARB_extensions_string	Supported
WGL_ARB_framebuffer_sRGB	Supported
WGL_ARB_make_current_read	Supported
WGL_ARB_multisample	Supported
WGL_ARB_pbuffer	Supported
WGL_ARB_pixel_format	Supported
WGL_ARB_pixel_format_float	Supported
WGL_ARB_render_texture	Not Supported
WGL_ARB_robustness_application_isolation	Not Supported
WGL_ARB_robustness_share_group_isolation	Not Supported
WGL_ATI_pbuffer_memory_hint	Not Supported
WGL_ATI_pixel_format_float	Not Supported
WGL_ATI_render_texture_rectangle	Not Supported
WGL_EXT_buffer_region	Not Supported
WGL_EXT_colorspace	Not Supported
WGL_EXT_create_context_es_profile	Supported
WGL_EXT_create_context_es2_profile	Supported
WGL_EXT_depth_float	Supported
WGL_EXT_display_color_table	Not Supported
WGL_EXT_extensions_string	Supported

Navigation

Navigation

WGL_EXT_framebuffer_sRGB	Not Supported
WGL_EXT_framebuffer_sRGBWGL_ARB_create_context	Not Supported
WGL_EXT_gamma_control	Not Supported
WGL_EXT_make_current_read	Not Supported
WGL_EXT_multisample	Not Supported
WGL_EXT_pbuffer	Not Supported
WGL_EXT_pixel_format	Not Supported
WGL_EXT_pixel_format_packed_float	Supported
WGL_EXT_render_texture	Not Supported
WGL_EXT_swap_control	Supported
WGL_EXT_swap_control_tear	Supported
WGL_EXT_swap_interval	Not Supported
WGL_I3D_digital_video_control	Not Supported
WGL_I3D_gamma	Not Supported
WGL_I3D_genlock	Not Supported
WGL_I3D_image_buffer	Not Supported
WGL_I3D_swap_frame_lock	Not Supported
WGL_I3D_swap_frame_usage	Not Supported
WGL_INTEL_cl_sharing	Not Supported
WGL_MTX_video_preview	Not Supported
WGL_NV_bridged_display	Not Supported
WGL_NV_copy_image	Not Supported
WGL_NV_delay_before_swap	Not Supported
WGL_NV_DX_interop	Supported
WGL_NV_DX_interop2	Not Supported
WGL_NV_float_buffer	Not Supported
WGL_NV_gpu_affinity	Not Supported
WGL_NV_multisample_coverage	Not Supported
WGL_NV_present_video	Not Supported
WGL_NV_render_depth_texture	Not Supported
WGL_NV_render_texture_rectangle	Not Supported
WGL_NV_swap_group	Not Supported
WGL_NV_texture_rectangle	Not Supported
WGL_NV_vertex_array_range	Not Supported
WGL_NV_video_capture	Not Supported
WGL_NV_video_output	Not Supported
WGL_NVX_DX_interop	Not Supported
WGL_OML_sync_control	Not Supported
WGL_S3_cl_sharingWGL_ARB_create_context_profile	Not Supported

Supported Compressed Texture Formats:

RGB DXT1	Supported
RGBA DXT1	Supported
RGBA DXT3	Supported
RGBA DXT5	Supported
RGB FXT1	Supported
RGBA FXT1	Supported
3Dc	Not Supported

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

GPGPU

[Direct3D: Intel(R) HD Graphics (IVB-DT GT1)]

Device Properties:

Device Name	Intel(R) HD Graphics
GPU Code Name	IVB-DT GT1
PCI Device	8086-0152 / 10CF-176D (Rev 09)
Dedicated Memory	32 MB
Driver Name	igdumdim32.dll
Driver Version	10.18.10.5129
Shader Model	SM 5.0
Max Threads	1024
Multiple UAV Access	8 UAVs
Thread Dispatch	3D
Thread Local Storage	32 KB

Device Features:

10-bit Precision Floating-Point	Not Supported
16-bit Precision Floating-Point	Not Supported
Append/Consume Buffers	Supported
Atomic Operations	Supported
Double-Precision Floating-Point	Supported
Gather4	Supported
Indirect Compute Dispatch	Supported
Map On Default Buffers	Supported

Device Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[OpenCL: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz]

OpenCL Properties:

Platform Name	Intel(R) OpenCL
Platform Vendor	Intel(R) Corporation
Platform Version	OpenCL 1.2
Platform Profile	Full

Device Properties:

Device Name	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
Device Type	CPU
Device Vendor	Intel(R) Corporation
Device Version	OpenCL 1.2 (Build 76427)
Device Profile	Full
Driver Version	3.0.1.10891
OpenCL C Version	OpenCL C 1.2
Clock Rate	3299 MHz
Compute Units	4

Navigation

Address Space Size	32-bit
Max 2D Image Size	16384 x 16384
Max 3D Image Size	2048 x 2048 x 2048
Max Image Array Size	2048
Max Image Buffer Size	33552384
Max Samplers	480
Max Work-Item Size	1024 x 1024 x 1024
Max Work-Group Size	1024
Max Argument Size	3840 bytes
Max Constant Buffer Size	128 KB
Max Constant Arguments	480
Max Printf Buffer Size	1 MB
Native ISA Vector Widths	char16, short8, int2, float8, double4
Preferred Native Vector Widths	char1, short1, int1, long1, float1, double1
Profiling Timer Resolution	100 ns
OpenCL DLL	opencl.dll (1.2.11.0)

Memory Properties:

Global Memory	2047 MB
Global Memory Cache	256 KB (Read/Write, 64-byte line)
Local Memory	32 KB
Max Memory Object Allocation Size	524256 KB
Memory Base Address Alignment	1024-bit
Min Data Type Alignment	128 bytes

OpenCL Compliancy:

OpenCL 1.1	Yes (100%)
OpenCL 1.2	Yes (100%)
OpenCL 2.0	No (62%)

Device Features:

Command-Queue Out Of Order Execution	Enabled
Command-Queue Profiling	Enabled
Compiler Available	Yes
Error Correction	Not Supported
Images	Supported
Kernel Execution	Supported
Linker Available	Yes
Little-Endian Device	Yes
Native Kernel Execution	Supported
Sub-Group Independent Forward Progress	Not Supported
SVM Atomics	Not Supported
SVM Coarse Grain Buffer	Not Supported
SVM Fine Grain Buffer	Not Supported
SVM Fine Grain System	Not Supported
Thread Trace	Not Supported
Unified Memory	Yes

Half-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Not Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Not Supported

Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Navigation

Single-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Supported
Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Double-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Supported
IEEE754-2008 FMA	Supported
INF and NaNs	Supported
Rounding to Infinity	Supported
Rounding to Nearest Even	Supported
Rounding to Zero	Supported
Software Basic Floating-Point Operations	No

Device Extensions:

Total / Supported Extensions	116 / 14
cl_altera_compiler_mode	Not Supported
cl_altera_device_temperature	Not Supported
cl_altera_live_object_tracking	Not Supported
cl_amd_bus_addressable_memory	Not Supported
cl_amd_c1x_atomics	Not Supported
cl_amd_compile_options	Not Supported
cl_amd_copy_buffer_p2p	Not Supported
cl_amd_core_id	Not Supported
cl_amd_d3d10_interop	Not Supported
cl_amd_d3d9_interop	Not Supported
cl_amd_device_attribute_query	Not Supported
cl_amd_device_board_name	Not Supported
cl_amd_device_memory_flags	Not Supported
cl_amd_device_persistent_memory	Not Supported
cl_amd_device_profiling_timer_offset	Not Supported
cl_amd_device_topology	Not Supported
cl_amd_event_callback	Not Supported
cl_amd_fp64	Not Supported
cl_amd_hsa	Not Supported
cl_amd_image2d_from_buffer_read_only	Not Supported
cl_amd_liquid_flash	Not Supported
cl_amd_media_ops	Not Supported
cl_amd_media_ops2	Not Supported
cl_amd_offline_devices	Not Supported
cl_amd_popcnt	Not Supported
cl_amd_predefined_macros	Not Supported
cl_amd_printf	Not Supported
cl_amd_svm	Not Supported
cl_amd_vec3	Not Supported
cl_apple_contextloggingfunctions	Not Supported

cl_apple_gl_sharing	Not Supported
cl_apple_setmemobjectdestructor	Not Supported
cl_arm_core_id	Not Supported
cl_arm_import_memory	Not Supported
cl_arm_import_memory_dma_buf	Not Supported
cl_arm_import_memory_host	Not Supported
cl_arm_integer_dot_product_int8	Not Supported
cl_arm_non_uniform_work_group_size	Not Supported
cl_arm_printf	Not Supported
cl_arm_thread_limit_hint	Not Supported
cl_ext_atomic_counters_32	Not Supported
cl_ext_atomic_counters_64	Not Supported
cl_ext_device_fission	Supported
cl_ext_migrate_memobject	Not Supported
cl_intel_accelerator	Not Supported
cl_intel_advanced_motion_estimation	Not Supported
cl_intel_ctz	Not Supported
cl_intel_d3d11_nv12_media_sharing	Not Supported
cl_intel_device_partition_by_names	Not Supported
cl_intel_device_side_avc_motion_estimation	Not Supported
cl_intel_driver_diagnostics	Not Supported
cl_intel_dx9_media_sharing	Supported
cl_intel_exec_by_local_thread	Supported
cl_intel_media_block_io	Not Supported
cl_intel_motion_estimation	Not Supported
cl_intel_packed_yuv	Not Supported
cl_intel_planar_yuv	Not Supported
cl_intel_printf	Supported
cl_intel_required_subgroup_size	Not Supported
cl_intel_simultaneous_sharing	Not Supported
cl_intel_spirv_device_side_avc_motion_estimation	Not Supported
cl_intel_spirv_media_block_io	Not Supported
cl_intel_spirv_subgroups	Not Supported
cl_intel_subgroups	Not Supported
cl_intel_subgroups_short	Not Supported
cl_intel_thread_local_exec	Not Supported
cl_intel_unified_shared_memory_preview	Not Supported
cl_intel_va_api_media_sharing	Not Supported
cl_intel_vec_len_hint	Not Supported
cl_intel_visual_analytics	Not Supported
cl_khr_3d_image_writes	Not Supported
cl_khr_byte_addressable_store	Supported
cl_khr_context_abort	Not Supported
cl_khr_create_command_queue	Not Supported
cl_khr_d3d10_sharing	Not Supported
cl_khr_d3d11_sharing	Supported
cl_khr_depth_images	Not Supported
cl_khr_dx9_media_sharing	Supported
cl_khr_egl_event	Not Supported
cl_khr_egl_image	Not Supported
cl_khr_fp16	Not Supported
cl_khr_fp64	Supported
cl_khr_gl_depth_images	Not Supported
cl_khr_gl_event	Not Supported
cl_khr_gl_msaa_sharing	Not Supported

Navigation

Navigation

cl_khr_gl_sharing	Supported
cl_khr_global_int32_base_atomics	Supported
cl_khr_global_int32_extended_atomics	Supported
cl_khr_icd	Supported
cl_khr_il_program	Not Supported
cl_khr_image2d_from_buffer	Not Supported
cl_khr_initialize_memory	Not Supported
cl_khr_int64_base_atomics	Not Supported
cl_khr_int64_extended_atomics	Not Supported
cl_khr_local_int32_base_atomics	Supported
cl_khr_local_int32_extended_atomics	Supported
cl_khr_mipmap_image	Not Supported
cl_khr_mipmap_image_writes	Not Supported
cl_khr_priority_hints	Not Supported
cl_khr_select_fprounding_mode	Not Supported
cl_khr_spir	Not Supported
cl_khr_spirv_no_integer_wrap_decoration	Not Supported
cl_khr_srgb_image_writes	Not Supported
cl_khr_subgroups	Not Supported
cl_khr_terminate_context	Not Supported
cl_khr_throttle_hints	Not Supported
cl_nv_compiler_options	Not Supported
cl_nv_copy_opts	Not Supported
cl_nv_create_buffer	Not Supported
cl_nv_d3d10_sharing	Not Supported
cl_nv_d3d11_sharing	Not Supported
cl_nv_d3d9_sharing	Not Supported
cl_nv_device_attribute_query	Not Supported
cl_nv_pragma_unroll	Not Supported
cl_qcom_ext_host_ptr	Not Supported
cl_qcom_ion_host_ptr	Not Supported

Device Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[OpenCL: Intel(R) HD Graphics 2500 (IVB-DT GT1)]

OpenCL Properties:

Platform Name	Intel(R) OpenCL
Platform Vendor	Intel(R) Corporation
Platform Version	OpenCL 1.2
Platform Profile	Full

Device Properties:

Device Name	Intel(R) HD Graphics 2500
GPU Code Name	IVB-DT GT1
Device Type	GPU
Device Vendor	Intel(R) Corporation
Device Version	OpenCL 1.2
Device Profile	Full
Driver Version	10.18.10.5129
OpenCL C Version	OpenCL C 1.2

Supported Built-In Kernels	block_motion_estimate_intel
Clock Rate	1050 MHz
Compute Units / Cores	6 / 24
Address Space Size	64-bit
Max 2D Image Size	16384 x 16384
Max 3D Image Size	2048 x 2048 x 2048
Max Image Array Size	2048
Max Image Buffer Size	22937600
Max Samplers	16
Max Work-Item Size	256 x 256 x 256
Max Work-Group Size	256
Max Argument Size	1 KB
Max Constant Buffer Size	64 KB
Max Constant Arguments	8
Max Printf Buffer Size	4 MB
Native ISA Vector Widths	char1, short1, int1, float1
Preferred Native Vector Widths	char1, short1, int1, long1, float1
Profiling Timer Resolution	80 ns
OpenCL DLL	opencl.dll (1.2.11.0)

Memory Properties:

Global Memory	1400 MB
Global Memory Cache	2048 KB (Read/Write, 64-byte line)
Local Memory	64 KB
Max Memory Object Allocation Size	350 MB
Memory Base Address Alignment	1024-bit
Min Data Type Alignment	128 bytes
Image Row Pitch Alignment	64 pixels
Image Base Address Alignment	4096 pixels

OpenCL Compliancy:

OpenCL 1.1	Yes (100%)
OpenCL 1.2	Yes (100%)
OpenCL 2.0	Yes (100%)

Device Features:

Command-Queue Out Of Order Execution	Disabled
Command-Queue Profiling	Enabled
Compiler Available	Yes
Error Correction	Not Supported
Images	Supported
Kernel Execution	Supported
Linker Available	Yes
Little-Endian Device	Yes
Native Kernel Execution	Not Supported
Sub-Group Independent Forward Progress	Not Supported
SVM Atomics	Not Supported
SVM Coarse Grain Buffer	Not Supported
SVM Fine Grain Buffer	Not Supported
SVM Fine Grain System	Not Supported
Thread Trace	Not Supported
Unified Memory	Yes

Half-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported

Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Not Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Not Supported
Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Single-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Supported
Rounding to Infinity	Supported
Rounding to Nearest Even	Supported
Rounding to Zero	Supported
Software Basic Floating-Point Operations	No

Double-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Not Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Not Supported
Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Device Extensions:

Total / Supported Extensions	116 / 20
cl_altera_compiler_mode	Not Supported
cl_altera_device_temperature	Not Supported
cl_altera_live_object_tracking	Not Supported
cl_amd_bus_addressable_memory	Not Supported
cl_amd_c1x_atomics	Not Supported
cl_amd_compile_options	Not Supported
cl_amd_copy_buffer_p2p	Not Supported
cl_amd_core_id	Not Supported
cl_amd_d3d10_interop	Not Supported
cl_amd_d3d9_interop	Not Supported
cl_amd_device_attribute_query	Not Supported
cl_amd_device_board_name	Not Supported
cl_amd_device_memory_flags	Not Supported
cl_amd_device_persistent_memory	Not Supported
cl_amd_device_profiling_timer_offset	Not Supported
cl_amd_device_topology	Not Supported
cl_amd_event_callback	Not Supported
cl_amd_fp64	Not Supported
cl_amd_hsa	Not Supported
cl_amd_image2d_from_buffer_read_only	Not Supported
cl_amd_liquid_flash	Not Supported
cl_amd_media_ops	Not Supported
cl_amd_media_ops2	Not Supported
cl_amd_offline_devices	Not Supported
cl_amd_popcnt	Not Supported

Navigation

cl_amd_predefined_macros	Not Supported
cl_amd_printf	Not Supported
cl_amd_svm	Not Supported
cl_amd_vec3	Not Supported
cl_apple_contextloggingfunctions	Not Supported
cl_apple_gl_sharing	Not Supported
cl_apple_setmemobjectdestructor	Not Supported
cl_arm_core_id	Not Supported
cl_arm_import_memory	Not Supported
cl_arm_import_memory_dma_buf	Not Supported
cl_arm_import_memory_host	Not Supported
cl_arm_integer_dot_product_int8	Not Supported
cl_arm_non_uniform_work_group_size	Not Supported
cl_arm_printf	Not Supported
cl_arm_thread_limit_hint	Not Supported
cl_ext_atomic_counters_32	Not Supported
cl_ext_atomic_counters_64	Not Supported
cl_ext_device_fission	Not Supported
cl_ext_migrate_memobject	Not Supported
cl_intel_accelerator	Supported
cl_intel_advanced_motion_estimation	Not Supported
cl_intel_ctz	Not Supported
cl_intel_d3d11_nv12_media_sharing	Supported
cl_intel_device_partition_by_names	Not Supported
cl_intel_device_side_avc_motion_estimation	Not Supported
cl_intel_driver_diagnostics	Not Supported
cl_intel_dx9_media_sharing	Supported
cl_intel_exec_by_local_thread	Not Supported
cl_intel_media_block_io	Not Supported
cl_intel_motion_estimation	Supported
cl_intel_packed_yuv	Not Supported
cl_intel_planar_yuv	Not Supported
cl_intel_printf	Not Supported
cl_intel_required_subgroup_size	Not Supported
cl_intel_simultaneous_sharing	Not Supported
cl_intel_spirv_device_side_avc_motion_estimation	Not Supported
cl_intel_spirv_media_block_io	Not Supported
cl_intel_spirv_subgroups	Not Supported
cl_intel_subgroups	Not Supported
cl_intel_subgroups_short	Not Supported
cl_intel_thread_local_exec	Not Supported
cl_intel_unified_shared_memory_preview	Not Supported
cl_intel_va_api_media_sharing	Not Supported
cl_intel_vec_len_hint	Not Supported
cl_intel_visual_analytics	Not Supported
cl_khr_3d_image_writes	Supported
cl_khr_byte_addressable_store	Supported
cl_khr_context_abort	Not Supported
cl_khr_create_command_queue	Not Supported
cl_khr_d3d10_sharing	Supported
cl_khr_d3d11_sharing	Supported
cl_khr_depth_images	Supported
cl_khr_dx9_media_sharing	Supported
cl_khr_egl_event	Not Supported
cl_khr_egl_image	Not Supported

Navigation

Navigation

cl_khr_fp16	Not Supported
cl_khr_fp64	Not Supported
cl_khr_gl_depth_images	Supported
cl_khr_gl_event	Supported
cl_khr_gl_msaa_sharing	Supported
cl_khr_gl_sharing	Supported
cl_khr_global_int32_base_atomics	Supported
cl_khr_global_int32_extended_atomics	Supported
cl_khr_icd	Supported
cl_khr_il_program	Not Supported
cl_khr_image2d_from_buffer	Supported
cl_khr_initialize_memory	Not Supported
cl_khr_int64_base_atomics	Not Supported
cl_khr_int64_extended_atomics	Not Supported
cl_khr_local_int32_base_atomics	Supported
cl_khr_local_int32_extended_atomics	Supported
cl_khr_mipmap_image	Not Supported
cl_khr_mipmap_image_writes	Not Supported
cl_khr_priority_hints	Not Supported
cl_khr_select_fprounding_mode	Not Supported
cl_khr_spir	Not Supported
cl_khr_spirv_no_integer_wrap_decoration	Not Supported
cl_khr_srgb_image_writes	Not Supported
cl_khr_subgroups	Not Supported
cl_khr_terminate_context	Not Supported
cl_khr_throttle_hints	Not Supported
cl_nv_compiler_options	Not Supported
cl_nv_copy_opts	Not Supported
cl_nv_create_buffer	Not Supported
cl_nv_d3d10_sharing	Not Supported
cl_nv_d3d11_sharing	Not Supported
cl_nv_d3d9_sharing	Not Supported
cl_nv_device_attribute_query	Not Supported
cl_nv_pragma_unroll	Not Supported
cl_qcom_ext_host_ptr	Not Supported
cl_qcom_ion_host_ptr	Not Supported

Device Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Fonts

Font Family	Type	Style	Character Set	Char. Size	Char. Weight
@Malgun Gothic Semilight	Swiss	Regular	Baltic	31 x 43	30 %
@Malgun Gothic Semilight	Swiss	Regular	CHINESE_BIG5	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
@Malgun Gothic Semilight	Swiss	Regular	Cyrillic	31 x 43	30 %
@Malgun Gothic Semilight	Swiss	Regular	Greek	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
@Malgun Gothic Semilight	Swiss	Regular	Hangul	31 x 43	30 %

@Malgun Gothic Semilight	Swiss	Regular	Hebrew	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
@Malgun Gothic Semilight	Swiss	Regular	Turkish	31 x 43	30 %
@Malgun Gothic Semilight	Swiss	Regular	Vietnamese	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
@Malgun Gothic	Swiss	Regular	Hangul	15 x 43	40 %
@Malgun Gothic	Swiss	Regular	Western	15 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Greek	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Western	32 x 43	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Greek	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Western	32 x 41	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	40 %
@Microsoft JhengHei UI	Swiss	Regular	Greek	15 x 41	40 %
@Microsoft JhengHei UI	Swiss	Regular	Western	15 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 43	40 %
@Microsoft JhengHei	Swiss	Regular	Greek	15 x 43	40 %
@Microsoft JhengHei	Swiss	Regular	Western	15 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	CHINESE_GB2312	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	Cyrillic	15 x 41	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	Turkish	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	Western	15 x 41	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	CHINESE_GB2312	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Cyrillic	15 x 42	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Turkish	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Western	15 x 42	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	CHINESE_GB2312	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Cyrillic	15 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Turkish	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Western	15 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	CHINESE_GB2312	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	Cyrillic	15 x 42	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	Turkish	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	Western	15 x 42	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
@MingLiU_HKSCS-ExtB	Roman	Regular	Western	16 x 32	40 %
@MingLiU-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
@MS Gothic	Modern	Regular	Baltic	16 x 32	40 %
@MS Gothic	Modern	Regular	Central European	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
@MS Gothic	Modern	Regular	Greek	16 x 32	40 %
@MS Gothic	Modern	Regular	Japanese	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
@MS Gothic	Modern	Regular	Western	16 x 32	40 %
@MS PGothic	Swiss	Regular	Baltic	13 x 32	40 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
@MS PGothic	Swiss	Regular	Cyrillic	13 x 32	40 %
@MS PGothic	Swiss	Regular	Greek	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
@MS PGothic	Swiss	Regular	Turkish	13 x 32	40 %
@MS PGothic	Swiss	Regular	Western	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Central European	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Cyrillic	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Japanese	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Turkish	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
@NSimSun	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@NSimSun	Modern	Regular	Western	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
@PMingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
@SimSun	Special	Regular	CHINESE_GB2312	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
@SimSun-ExtB	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@SimSun-ExtB	Modern	Regular	Western	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Central European	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Cyrillic	31 x 41	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Japanese	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Turkish	31 x 41	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	30 %
@Yu Gothic Medium	Swiss	Regular	Baltic	31 x 41	50 %
@Yu Gothic Medium	Swiss	Regular	Central European	31 x 41	50 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	50 %
@Yu Gothic Medium	Swiss	Regular	Greek	31 x 41	50 %
@Yu Gothic Medium	Swiss	Regular	Japanese	31 x 41	50 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	50 %
@Yu Gothic Medium	Swiss	Regular	Western	31 x 41	50 %
@Yu Gothic UI Light	Swiss	Regular	Baltic	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
@Yu Gothic UI Light	Swiss	Regular	Cyrillic	17 x 43	30 %
@Yu Gothic UI Light	Swiss	Regular	Greek	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
@Yu Gothic UI Light	Swiss	Regular	Turkish	17 x 43	30 %
@Yu Gothic UI Light	Swiss	Regular	Western	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	60 %
@Yu Gothic UI Semibold	Swiss	Regular	Central European	19 x 43	60 %
@Yu Gothic UI Semibold	Swiss	Regular	Cyrillic	19 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	60 %
@Yu Gothic UI Semibold	Swiss	Regular	Japanese	19 x 43	60 %
@Yu Gothic UI Semibold	Swiss	Regular	Turkish	19 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	60 %
@Yu Gothic UI Semilight	Swiss	Regular	Baltic	17 x 43	35 %
@Yu Gothic UI Semilight	Swiss	Regular	Central European	17 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	35 %
@Yu Gothic UI Semilight	Swiss	Regular	Greek	17 x 43	35 %
@Yu Gothic UI Semilight	Swiss	Regular	Japanese	17 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	35 %

Navigation

@Yu Gothic UI Semilight	Swiss	Regular	Western	17 x 43	35 %
@Yu Gothic UI	Swiss	Regular	Baltic	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
@Yu Gothic UI	Swiss	Regular	Cyrillic	17 x 43	40 %
@Yu Gothic UI	Swiss	Regular	Greek	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
@Yu Gothic UI	Swiss	Regular	Turkish	17 x 43	40 %
@Yu Gothic UI	Swiss	Regular	Western	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Central European	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Cyrillic	31 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Japanese	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Turkish	31 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	40 %
AcadEref	Special	Regular	Western	39 x 33	40 %
Agency FB	Swiss	Regular	Western	10 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	33 x 48	40 %
Algerian	Decorative	Regular	Western	17 x 36	40 %
AmdtSymbols	Special	Regular	Western	40 x 25	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	32 x 48	40 %
Arial Black	Swiss	Regular	Baltic	18 x 45	90 %
Arial Black	Swiss	Regular	Central European	18 x 45	90 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	90 %
Arial Black	Swiss	Regular	Greek	18 x 45	90 %
Arial Black	Swiss	Regular	Turkish	18 x 45	90 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	90 %
Arial Narrow	Swiss	Regular	Baltic	12 x 36	40 %
Arial Narrow	Swiss	Regular	Central European	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Arial Narrow	Swiss	Regular	Greek	12 x 36	40 %
Arial Narrow	Swiss	Regular	Turkish	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Arial Rounded MT Bold	Swiss	Regular	Western	15 x 37	40 %
Arial	Swiss	Regular	Arabic	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Arial	Swiss	Regular	Central European	14 x 36	40 %
Arial	Swiss	Regular	Cyrillic	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Arial	Swiss	Regular	Hebrew	14 x 36	40 %
Arial	Swiss	Regular	Turkish	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Arial	Swiss	Regular	Western	14 x 36	40 %
Bahnschrift Condensed	Swiss	Condensed	Baltic	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift Condensed	Swiss	Condensed	Cyrillic	18 x 38	40 %
Bahnschrift Condensed	Swiss	Condensed	Greek	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift Condensed	Swiss	Condensed	Vietnamese	18 x 38	40 %
Bahnschrift Condensed	Swiss	Condensed	Western	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light Condensed	Swiss	Light Condensed	Central European	18 x 38	30 %
Bahnschrift Light Condensed	Swiss	Light Condensed	Cyrillic	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light Condensed	Swiss	Light Condensed	Turkish	18 x 38	30 %

Navigation

Bahnschrift Light Condensed	Swiss	Light Condensed	Vietnamese	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light SemiCondensed	Swiss	Light SemiCondensed	Baltic	18 x 38	30 %
Bahnschrift Light SemiCondensed	Swiss	Light SemiCondensed	Central European	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light SemiCondensed	Swiss	Light SemiCondensed	Greek	18 x 38	30 %
Bahnschrift Light SemiCondensed	Swiss	Light SemiCondensed	Turkish	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light SemiCondensed	Swiss	Light SemiCondensed	Western	18 x 38	30 %
Bahnschrift Light	Swiss	Light	Baltic	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light	Swiss	Light	Cyrillic	18 x 38	30 %
Bahnschrift Light	Swiss	Light	Greek	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	30 %
Bahnschrift Light	Swiss	Light	Vietnamese	18 x 38	30 %
Bahnschrift Light	Swiss	Light	Western	18 x 38	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold Condensed	Swiss	SemiBold Condensed	Central European	18 x 38	60 %
Bahnschrift SemiBold Condensed	Swiss	SemiBold Condensed	Cyrillic	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold Condensed	Swiss	SemiBold Condensed	Turkish	18 x 38	60 %
Bahnschrift SemiBold Condensed	Swiss	SemiBold Condensed	Vietnamese	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold SemiConden	Swiss	SemiBold SemiCondensed	Baltic	18 x 38	60 %
Bahnschrift SemiBold SemiConden	Swiss	SemiBold SemiCondensed	Central European	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold SemiConden	Swiss	SemiBold SemiCondensed	Greek	18 x 38	60 %
Bahnschrift SemiBold SemiConden	Swiss	SemiBold SemiCondensed	Turkish	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold SemiConden	Swiss	SemiBold SemiCondensed	Western	18 x 38	60 %
Bahnschrift SemiBold	Swiss	SemiBold	Baltic	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold	Swiss	SemiBold	Cyrillic	18 x 38	60 %
Bahnschrift SemiBold	Swiss	SemiBold	Greek	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	60 %
Bahnschrift SemiBold	Swiss	SemiBold	Vietnamese	18 x 38	60 %
Bahnschrift SemiBold	Swiss	SemiBold	Western	18 x 38	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift SemiCondensed	Swiss	SemiCondensed	Central European	18 x 38	40 %
Bahnschrift SemiCondensed	Swiss	SemiCondensed	Cyrillic	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift SemiCondensed	Swiss	SemiCondensed	Turkish	18 x 38	40 %
Bahnschrift SemiCondensed	Swiss	SemiCondensed	Vietnamese	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift SemiLight Condensed	Swiss	SemiLight Condensed	Baltic	18 x 38	35 %
Bahnschrift SemiLight Condensed	Swiss	SemiLight Condensed	Central European	18 x 38	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift SemiLight Condensed	Swiss	SemiLight Condensed	Greek	18 x 38	35 %
Bahnschrift SemiLight Condensed	Swiss	SemiLight Condensed	Turkish	18 x 38	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift SemiLight Condensed	Swiss	SemiLight Condensed	Western	18 x 38	35 %
Bahnschrift SemiLight SemiConde	Swiss	SemiLight SemiCondensed	Baltic	18 x 38	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift SemiLight SemiConde	Swiss	SemiLight SemiCondensed	Cyrillic	18 x 38	35 %
Bahnschrift SemiLight SemiConde	Swiss	SemiLight SemiCondensed	Greek	18 x 38	35 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift SemiLight SemiConde	Swiss	SemiLight SemiCondensed	Vietnamese	18 x 38	35 %
Bahnschrift SemiLight SemiConde	Swiss	SemiLight SemiCondensed	Western	18 x 38	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift SemiLight	Swiss	SemiLight	Central European	18 x 38	35 %
Bahnschrift SemiLight	Swiss	SemiLight	Cyrillic	18 x 38	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift SemiLight	Swiss	SemiLight	Turkish	18 x 38	35 %
Bahnschrift SemiLight	Swiss	SemiLight	Vietnamese	18 x 38	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	35 %
Bahnschrift	Swiss	Regular	Baltic	18 x 38	40 %
Bahnschrift	Swiss	Regular	Central European	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift	Swiss	Regular	Greek	18 x 38	40 %
Bahnschrift	Swiss	Regular	Turkish	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Bahnschrift	Swiss	Regular	Western	18 x 38	40 %
BankGothic Lt BT	Swiss	Light	Central European	18 x 33	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 33	40 %
BankGothic Lt BT	Swiss	Light	Mac	18 x 33	40 %
BankGothic Lt BT	Swiss	Light	Turkish	18 x 33	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 33	40 %
BankGothic Md BT	Swiss	Medium	Central European	19 x 34	40 %
BankGothic Md BT	Swiss	Medium	Greek	19 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 34	40 %
BankGothic Md BT	Swiss	Medium	Turkish	19 x 34	40 %
BankGothic Md BT	Swiss	Medium	Western	19 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 37	40 %
Bauhaus 93	Decorative	Regular	Western	14 x 36	40 %
Bell MT	Roman	Regular	Western	13 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	70 %
Berlin Sans FB	Swiss	Regular	Western	13 x 35	40 %
Bernard MT Condensed	Roman	Regular	Western	12 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 41	40 %
Bodoni MT Black	Roman	Regular	Western	16 x 37	90 %
Bodoni MT Condensed	Roman	Regular	Western	9 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	8 x 37	30 %
Bodoni MT Poster Compressed	Roman	Regular	Western	8 x 37	30 %
Bodoni MT	Roman	Regular	Western	13 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 40	40 %
Book Antiqua	Roman	Regular	Central European	14 x 40	40 %
Book Antiqua	Roman	Regular	Cyrillic	14 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 40	40 %
Book Antiqua	Roman	Regular	Turkish	14 x 40	40 %
Book Antiqua	Roman	Regular	Western	14 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 36	30 %
Bookman Old Style	Roman	Regular	Central European	16 x 36	30 %
Bookman Old Style	Roman	Regular	Cyrillic	16 x 36	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 36	30 %
Bookman Old Style	Roman	Regular	Turkish	16 x 36	30 %
Bookman Old Style	Roman	Regular	Western	16 x 36	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 32	40 %
Bradley Hand ITC	Script	Regular	Western	13 x 40	40 %
Britannic Bold	Swiss	Regular	Western	14 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 36	40 %

Navigation

Brush Script MT	Script	Italic	Western	10 x 39	40 %
Calibri Light	Swiss	Regular	Arabic	17 x 39	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	30 %
Calibri Light	Swiss	Regular	Central European	17 x 39	30 %
Calibri Light	Swiss	Regular	Cyrillic	17 x 39	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	30 %
Calibri Light	Swiss	Regular	Hebrew	17 x 39	30 %
Calibri Light	Swiss	Regular	Turkish	17 x 39	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	30 %
Calibri Light	Swiss	Regular	Western	17 x 39	30 %
Calibri	Swiss	Regular	Arabic	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Calibri	Swiss	Regular	Central European	17 x 39	40 %
Calibri	Swiss	Regular	Cyrillic	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Calibri	Swiss	Regular	Hebrew	17 x 39	40 %
Calibri	Swiss	Regular	Turkish	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Calibri	Swiss	Regular	Western	17 x 39	40 %
Californian FB	Roman	Regular	Western	13 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 37	40 %
Cambria Math	Roman	Regular	Baltic	20 x 179	40 %
Cambria Math	Roman	Regular	Central European	20 x 179	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 179	40 %
Cambria Math	Roman	Regular	Greek	20 x 179	40 %
Cambria Math	Roman	Regular	Turkish	20 x 179	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 179	40 %
Cambria Math	Roman	Regular	Western	20 x 179	40 %
Cambria	Roman	Regular	Baltic	20 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 38	40 %
Cambria	Roman	Regular	Cyrillic	20 x 38	40 %
Cambria	Roman	Regular	Greek	20 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 38	40 %
Cambria	Roman	Regular	Vietnamese	20 x 38	40 %
Cambria	Roman	Regular	Western	20 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Candara Light	Swiss	Regular	Central European	17 x 39	40 %
Candara Light	Swiss	Regular	Cyrillic	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Candara Light	Swiss	Regular	Turkish	17 x 39	40 %
Candara Light	Swiss	Regular	Vietnamese	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Candara	Swiss	Regular	Baltic	17 x 39	40 %
Candara	Swiss	Regular	Central European	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Candara	Swiss	Regular	Greek	17 x 39	40 %
Candara	Swiss	Regular	Turkish	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Candara	Swiss	Regular	Western	17 x 39	40 %
Castellar	Roman	Regular	Western	21 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Century Gothic	Swiss	Regular	Baltic	16 x 38	40 %
Century Gothic	Swiss	Regular	Central European	16 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 38	40 %
Century Gothic	Swiss	Regular	Greek	16 x 38	40 %

Navigation

Century Gothic	Swiss	Regular	Turkish	16 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 38	40 %
Century Schoolbook	Roman	Regular	Baltic	15 x 38	40 %
Century Schoolbook	Roman	Regular	Central European	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 38	40 %
Century Schoolbook	Roman	Regular	Greek	15 x 38	40 %
Century Schoolbook	Roman	Regular	Turkish	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 38	40 %
Century	Roman	Regular	Baltic	15 x 38	40 %
Century	Roman	Regular	Central European	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 38	40 %
Century	Roman	Regular	Greek	15 x 38	40 %
Century	Roman	Regular	Turkish	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 38	40 %
Chiller	Decorative	Regular	Western	9 x 37	40 %
CityBlueprint	Special	Regular	Symbol	11 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 34	40 %
Comic Sans MS	Script	Regular	Baltic	15 x 45	40 %
Comic Sans MS	Script	Regular	Central European	15 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 45	40 %
Comic Sans MS	Script	Regular	Greek	15 x 45	40 %
Comic Sans MS	Script	Regular	Turkish	15 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 45	40 %
CommercialPi BT	Roman	Regular	Symbol	22 x 32	40 %
CommercialScript BT	Script	Regular	Central European	12 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 37	40 %
CommercialScript BT	Script	Regular	Mac	12 x 37	40 %
CommercialScript BT	Script	Regular	Turkish	12 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 37	40 %
Complex	Special	Regular	Arabic	22 x 45	40 %
Complex	Special	Regular	Baltic	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
Complex	Special	Regular	Cyrillic	22 x 45	40 %
Complex	Special	Regular	Greek	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
Complex	Special	Regular	Turkish	22 x 45	40 %
Complex	Special	Regular	Vietnamese	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
Consolas	Modern	Regular	Baltic	18 x 37	40 %
Consolas	Modern	Regular	Central European	18 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 37	40 %
Consolas	Modern	Regular	Greek	18 x 37	40 %
Consolas	Modern	Regular	Turkish	18 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 37	40 %
Consolas	Modern	Regular	Western	18 x 37	40 %
Constantia	Roman	Regular	Baltic	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Constantia	Roman	Regular	Cyrillic	17 x 39	40 %
Constantia	Roman	Regular	Greek	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Constantia	Roman	Regular	Vietnamese	17 x 39	40 %
Constantia	Roman	Regular	Western	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 37	40 %
Copperplate Gothic Bold	Swiss	Regular	Western	19 x 36	40 %
Copperplate Gothic Light	Swiss	Regular	Western	18 x 35	40 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	30 %
Corbel Light	Swiss	Regular	Central European	16 x 39	30 %
Corbel Light	Swiss	Regular	Cyrillic	16 x 39	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	30 %
Corbel Light	Swiss	Regular	Turkish	16 x 39	30 %
Corbel Light	Swiss	Regular	Vietnamese	16 x 39	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	30 %
Corbel	Swiss	Regular	Baltic	17 x 39	40 %
Corbel	Swiss	Regular	Central European	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Corbel	Swiss	Regular	Greek	17 x 39	40 %
Corbel	Swiss	Regular	Turkish	17 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 39	40 %
Corbel	Swiss	Regular	Western	17 x 39	40 %
CountryBlueprint	Special	Regular	Symbol	13 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 36	40 %
Courier New	Modern	Regular	Baltic	19 x 36	40 %
Courier New	Modern	Regular	Central European	19 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 36	40 %
Courier New	Modern	Regular	Greek	19 x 36	40 %
Courier New	Modern	Regular	Hebrew	19 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 36	40 %
Courier New	Modern	Regular	Vietnamese	19 x 36	40 %
Courier New	Modern	Regular	Western	19 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	8 x 13	40 %
Curlz MT	Decorative	Regular	Western	12 x 42	40 %
Dubai Light	Swiss	Regular	Arabic	16 x 54	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 54	30 %
Dubai Medium	Swiss	Regular	Arabic	17 x 54	50 %
Dubai Medium	Swiss	Regular	Western	17 x 54	50 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 54	40 %
Dubai	Swiss	Regular	Western	16 x 54	40 %
Dutch801 Rm BT	Roman	Roman	Central European	14 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	40 %
Dutch801 Rm BT	Roman	Roman	Mac	14 x 39	40 %
Dutch801 Rm BT	Roman	Roman	Turkish	14 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	40 %
Dutch801 XBd BT	Roman	Extra Bold	Central European	15 x 39	40 %
Dutch801 XBd BT	Roman	Extra Bold	Greek	15 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 39	40 %
Dutch801 XBd BT	Roman	Extra Bold	Turkish	15 x 39	40 %
Dutch801 XBd BT	Roman	Extra Bold	Western	15 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	40 %
Ebrima	Special	Regular	Central European	19 x 43	40 %
Ebrima	Special	Regular	Turkish	19 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	40 %
Edwardian Script ITC	Script	Regular	Western	8 x 38	40 %
Elephant	Roman	Regular	Western	16 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 37	50 %
Eras Bold ITC	Swiss	Regular	Western	16 x 37	40 %
Eras Demi ITC	Swiss	Regular	Western	15 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 36	40 %
Eras Medium ITC	Swiss	Regular	Western	14 x 36	40 %
EuroRoman	Special	Regular	Symbol	13 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 37	40 %

Navigation

Fixedsys	Modern		Western	8 x 15	40 %
Footlight MT Light	Roman	Regular	Western	13 x 34	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 35	40 %
Franklin Gothic Book	Swiss	Regular	Baltic	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Central European	13 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Greek	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Turkish	13 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Baltic	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Central European	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Greek	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Turkish	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Baltic	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Central European	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Greek	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Turkish	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Baltic	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Central European	15 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Greek	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Turkish	15 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Baltic	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Central European	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Greek	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Turkish	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Baltic	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Central European	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Greek	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Turkish	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Freestyle Script	Script	Regular	Western	8 x 38	40 %
French Script MT	Script	Regular	Western	9 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 59	40 %
Gabriola	Decorative	Regular	Central European	16 x 59	40 %
Gabriola	Decorative	Regular	Cyrillic	16 x 59	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 59	40 %
Gabriola	Decorative	Regular	Turkish	16 x 59	40 %
Gabriola	Decorative	Regular	Western	16 x 59	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 43	40 %
Garamond	Roman	Regular	Baltic	12 x 36	40 %
Garamond	Roman	Regular	Central European	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
Garamond	Roman	Regular	Greek	12 x 36	40 %
Garamond	Roman	Regular	Turkish	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 36	40 %
GDT	Special	Regular	Western	41 x 48	40 %

Navigation

GENISO	Special	Regular	Arabic	17 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 51	40 %
GENISO	Special	Regular	Central European	17 x 51	40 %
GENISO	Special	Regular	Cyrillic	17 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 51	40 %
GENISO	Special	Regular	Hebrew	17 x 51	40 %
GENISO	Special	Regular	Turkish	17 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 51	40 %
GENISO	Special	Regular	Western	17 x 51	40 %
Georgia	Roman	Regular	Baltic	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Georgia	Roman	Regular	Cyrillic	14 x 36	40 %
Georgia	Roman	Regular	Greek	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Georgia	Roman	Regular	Western	14 x 36	40 %
Gigi	Decorative	Regular	Western	13 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 39	40 %
Gill Sans MT Condensed	Swiss	Regular	Western	10 x 39	40 %
Gill Sans MT Ext Condensed Bold	Swiss	Regular	Central European	7 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	7 x 38	40 %
Gill Sans MT	Swiss	Regular	Central European	13 x 37	40 %
Gill Sans MT	Swiss	Regular	Western	13 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 40	40 %
Gill Sans Ultra Bold Condensed	Swiss	Regular	Western	14 x 40	40 %
Gill Sans Ultra Bold	Swiss	Regular	Central European	20 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 40	40 %
Gloucester MT Extra Condensed	Roman	Regular	Western	9 x 37	40 %
GothicE	Special	Regular	Arabic	19 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 46	40 %
GothicE	Special	Regular	Central European	19 x 46	40 %
GothicE	Special	Regular	Cyrillic	19 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 46	40 %
GothicE	Special	Regular	Hebrew	19 x 46	40 %
GothicE	Special	Regular	Turkish	19 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 46	40 %
GothicE	Special	Regular	Western	19 x 46	40 %
GothicG	Special	Regular	Arabic	18 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	40 %
GothicG	Special	Regular	Central European	18 x 45	40 %
GothicG	Special	Regular	Cyrillic	18 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	40 %
GothicG	Special	Regular	Hebrew	18 x 45	40 %
GothicG	Special	Regular	Turkish	18 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	40 %
GothicG	Special	Regular	Western	18 x 45	40 %
GothicI	Special	Regular	Arabic	18 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	40 %
GothicI	Special	Regular	Central European	18 x 45	40 %
GothicI	Special	Regular	Cyrillic	18 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	40 %
GothicI	Special	Regular	Hebrew	18 x 45	40 %
GothicI	Special	Regular	Turkish	18 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 45	40 %
GothicI	Special	Regular	Western	18 x 45	40 %
Goudy Old Style	Roman	Regular	Western	13 x 36	40 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	36 x 44	40 %
GreekC	Special	Regular	Arabic	23 x 44	40 %
GreekC	Special	Regular	Baltic	23 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 44	40 %
GreekC	Special	Regular	Cyrillic	23 x 44	40 %
GreekC	Special	Regular	Greek	23 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 44	40 %
GreekC	Special	Regular	Turkish	23 x 44	40 %
GreekC	Special	Regular	Vietnamese	23 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 44	40 %
GreekS	Special	Regular	Arabic	22 x 46	40 %
GreekS	Special	Regular	Baltic	22 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 46	40 %
GreekS	Special	Regular	Cyrillic	22 x 46	40 %
GreekS	Special	Regular	Greek	22 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 46	40 %
GreekS	Special	Regular	Turkish	22 x 46	40 %
GreekS	Special	Regular	Vietnamese	22 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 46	40 %
Haettenschweiler	Swiss	Regular	Baltic	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Central European	10 x 33	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Greek	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Turkish	10 x 33	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 33	40 %
Harlow Solid Italic	Decorative	Italic	Western	12 x 40	40 %
Harrington	Decorative	Regular	Western	14 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 37	40 %
HoloLens MDL2 Assets	Roman	Regular	Western	34 x 32	40 %
Impact	Swiss	Regular	Baltic	19 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 39	40 %
Impact	Swiss	Regular	Cyrillic	19 x 39	40 %
Impact	Swiss	Regular	Greek	19 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 39	40 %
Impact	Swiss	Regular	Western	19 x 39	40 %
Imprint MT Shadow	Decorative	Regular	Western	13 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 32	40 %
Ink Free	Script	Regular	Western	17 x 40	40 %
ISOCP	Special	Regular	Arabic	16 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 51	40 %
ISOCP	Special	Regular	Central European	16 x 51	40 %
ISOCP	Special	Regular	Cyrillic	16 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 51	40 %
ISOCP	Special	Regular	Hebrew	16 x 51	40 %
ISOCP	Special	Regular	Turkish	16 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 51	40 %
ISOCP	Special	Regular	Western	16 x 51	40 %
ISOCP2	Special	Regular	Arabic	14 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 51	40 %
ISOCP2	Special	Regular	Central European	14 x 51	40 %
ISOCP2	Special	Regular	Cyrillic	14 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 51	40 %
ISOCP2	Special	Regular	Hebrew	14 x 51	40 %
ISOCP2	Special	Regular	Turkish	14 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 51	40 %

Navigation

ISOCP2	Special	Regular	Western	14 x 51	40 %
ISOCP3	Special	Regular	Arabic	14 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 51	40 %
ISOCP3	Special	Regular	Central European	14 x 51	40 %
ISOCP3	Special	Regular	Cyrillic	14 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 51	40 %
ISOCP3	Special	Regular	Hebrew	14 x 51	40 %
ISOCP3	Special	Regular	Turkish	14 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 51	40 %
ISOCP3	Special	Regular	Western	14 x 51	40 %
ISOCPEUR	Swiss	Regular	Baltic	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
ISOCPEUR	Swiss	Regular	Cyrillic	16 x 39	40 %
ISOCPEUR	Swiss	Regular	Greek	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
ISOCPEUR	Swiss	Regular	Western	16 x 39	40 %
ISOCT	Special	Regular	Arabic	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT	Special	Regular	Central European	25 x 55	40 %
ISOCT	Special	Regular	Cyrillic	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT	Special	Regular	Hebrew	25 x 55	40 %
ISOCT	Special	Regular	Turkish	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT	Special	Regular	Western	25 x 55	40 %
ISOCT2	Special	Regular	Arabic	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT2	Special	Regular	Central European	25 x 55	40 %
ISOCT2	Special	Regular	Cyrillic	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT2	Special	Regular	Hebrew	25 x 55	40 %
ISOCT2	Special	Regular	Turkish	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT2	Special	Regular	Western	25 x 55	40 %
ISOCT3	Special	Regular	Arabic	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT3	Special	Regular	Central European	25 x 55	40 %
ISOCT3	Special	Regular	Cyrillic	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT3	Special	Regular	Hebrew	25 x 55	40 %
ISOCT3	Special	Regular	Turkish	25 x 55	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 55	40 %
ISOCT3	Special	Regular	Western	25 x 55	40 %
ISOCTEUR	Modern	Regular	Baltic	23 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 39	40 %
ISOCTEUR	Modern	Regular	Cyrillic	23 x 39	40 %
ISOCTEUR	Modern	Regular	Greek	23 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 39	40 %
ISOCTEUR	Modern	Regular	Western	23 x 39	40 %
Italic	Special	Regular	Arabic	22 x 47	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 47	40 %
Italic	Special	Regular	Central European	22 x 47	40 %
Italic	Special	Regular	Cyrillic	22 x 47	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 47	40 %
Italic	Special	Regular	Hebrew	22 x 47	40 %

Navigation

Italic	Special	Regular	Turkish	22 x 47	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 47	40 %
Italic	Special	Regular	Western	22 x 47	40 %
ItalicC	Special	Regular	Arabic	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
ItalicC	Special	Regular	Central European	22 x 45	40 %
ItalicC	Special	Regular	Cyrillic	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
ItalicC	Special	Regular	Hebrew	22 x 45	40 %
ItalicC	Special	Regular	Turkish	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
ItalicC	Special	Regular	Western	22 x 45	40 %
ItalicT	Special	Regular	Arabic	22 x 48	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 48	40 %
ItalicT	Special	Regular	Central European	22 x 48	40 %
ItalicT	Special	Regular	Cyrillic	22 x 48	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 48	40 %
ItalicT	Special	Regular	Hebrew	22 x 48	40 %
ItalicT	Special	Regular	Turkish	22 x 48	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 48	40 %
ItalicT	Special	Regular	Western	22 x 48	40 %
Javanese Text	Special	Regular	Western	26 x 73	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 48	40 %
Juice ITC	Decorative	Regular	Western	9 x 36	40 %
Kristen ITC	Script	Regular	Western	16 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	8 x 35	40 %
Leelawadee UI Semilight	Swiss	Regular	Thai	17 x 43	35 %
Leelawadee UI Semilight	Swiss	Regular	Vietnamese	17 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	35 %
Leelawadee UI	Swiss	Regular	Thai	17 x 43	40 %
Leelawadee UI	Swiss	Regular	Vietnamese	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
Leelawadee	Swiss	Regular	Thai	17 x 38	40 %
Leelawadee	Swiss	Regular	Western	17 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 36	40 %
Lucida Calligraphy	Script	Italic	Western	17 x 40	40 %
Lucida Console	Modern	Regular	Central European	19 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 32	40 %
Lucida Console	Modern	Regular	Greek	19 x 32	40 %
Lucida Console	Modern	Regular	Turkish	19 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 32	40 %
Lucida Fax	Roman	Regular	Western	16 x 37	40 %
Lucida Handwriting	Script	Italic	Western	18 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 36	40 %
Lucida Sans Unicode	Swiss	Regular	Baltic	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Central European	16 x 49	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Greek	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Hebrew	16 x 49	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Western	16 x 49	40 %
Lucida Sans	Swiss	Regular	Western	16 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 39	70 %
Maiandra GD	Swiss	Regular	Western	14 x 38	40 %
Malgun Gothic Semilight	Swiss	Regular	Baltic	31 x 43	30 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	CHINESE_GB2312	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	Cyrillic	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	Hangul(Johab)	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	Hangul	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	Japanese	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	Turkish	31 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 43	30 %
Malgun Gothic Semilight	Swiss	Regular	Western	31 x 43	30 %
Malgun Gothic	Swiss	Regular	Hangul	15 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 43	40 %
Marlett	Special	Regular	Symbol	31 x 32	50 %
Matura MT Script Capitals	Script	Regular	Western	14 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
Microsoft JhengHei Light	Swiss	Regular	CHINESE_BIG5	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Greek	32 x 43	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	32 x 43	29 %
Microsoft JhengHei UI Light	Swiss	Regular	CHINESE_BIG5	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Greek	32 x 41	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	32 x 41	29 %
Microsoft JhengHei UI	Swiss	Regular	CHINESE_BIG5	15 x 41	40 %
Microsoft JhengHei UI	Swiss	Regular	Greek	15 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	40 %
Microsoft JhengHei	Swiss	Regular	CHINESE_BIG5	15 x 43	40 %
Microsoft JhengHei	Swiss	Regular	Greek	15 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 43	40 %
Microsoft New Tai Lue	Swiss	Regular	Western	19 x 42	40 %
Microsoft PhagsPa	Swiss	Regular	Western	24 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Baltic	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Central European	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Greek	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Hebrew	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Turkish	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Vietnamese	14 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 36	40 %
Microsoft Tai Le	Swiss	Regular	Western	19 x 41	40 %
Microsoft Uighur	Special	Regular	Arabic	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
Microsoft YaHei Light	Swiss	Regular	Central European	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	CHINESE_GB2312	15 x 41	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	Greek	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	Turkish	15 x 41	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	29 %
Microsoft YaHei UI Light	Swiss	Regular	Central European	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	CHINESE_GB2312	15 x 42	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	Greek	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	Turkish	15 x 42	29 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	29 %

Navigation

Microsoft YaHei UI	Swiss	Regular	Central European	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	CHINESE_GB2312	15 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	Greek	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	Turkish	15 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 41	40 %
Microsoft YaHei	Swiss	Regular	Central European	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	CHINESE_GB2312	15 x 42	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	Greek	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	Turkish	15 x 42	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 42	40 %
Microsoft Yi Baiti	Script	Regular	Western	21 x 32	40 %
MingLiU_HKSCS-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
MingLiU-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
MingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 39	40 %
Mistral	Script	Regular	Central European	10 x 39	40 %
Mistral	Script	Regular	Cyrillic	10 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 39	40 %
Mistral	Script	Regular	Turkish	10 x 39	40 %
Mistral	Script	Regular	Western	10 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 33	40 %
Modern	Modern		OEM/DOS	19 x 37	40 %
Mongolian Baiti	Script	Regular	Western	14 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 38	40 %
Monospac821 BT	Modern	Roman	Greek	19 x 38	40 %
Monospac821 BT	Modern	Roman	Mac	19 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 38	40 %
Monospac821 BT	Modern	Roman	Western	19 x 38	40 %
Monotxt	Special	Regular	Arabic	23 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 40	40 %
Monotxt	Special	Regular	Central European	23 x 40	40 %
Monotxt	Special	Regular	Cyrillic	23 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 40	40 %
Monotxt	Special	Regular	Hebrew	23 x 40	40 %
Monotxt	Special	Regular	Turkish	23 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 40	40 %
Monotxt	Special	Regular	Western	23 x 40	40 %
Monotype Corsiva	Script	Regular	Baltic	11 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	11 x 35	40 %
Monotype Corsiva	Script	Regular	Cyrillic	11 x 35	40 %
Monotype Corsiva	Script	Regular	Greek	11 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	11 x 35	40 %
Monotype Corsiva	Script	Regular	Western	11 x 35	40 %
MS Gothic	Modern	Regular	Baltic	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
MS Gothic	Modern	Regular	Cyrillic	16 x 32	40 %
MS Gothic	Modern	Regular	Greek	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
MS Gothic	Modern	Regular	Turkish	16 x 32	40 %
MS Gothic	Modern	Regular	Western	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 33	40 %
MS PGothic	Swiss	Regular	Baltic	13 x 32	40 %

Navigation

MS PGothic	Swiss	Regular	Central European	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
MS PGothic	Swiss	Regular	Greek	13 x 32	40 %
MS PGothic	Swiss	Regular	Japanese	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
MS PGothic	Swiss	Regular	Western	13 x 32	40 %
MS Reference Sans Serif	Swiss	Regular	Baltic	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Cyrillic	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Greek	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Vietnamese	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Western	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 39	40 %
MS Sans Serif	Swiss		Western	5 x 13	40 %
MS Serif	Roman		Western	5 x 13	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Central European	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Cyrillic	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Japanese	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Turkish	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
MT Extra	Roman	Regular	Symbol	20 x 32	40 %
MV Boli	Special	Regular	Western	18 x 52	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 60	40 %
Niagara Engraved	Decorative	Regular	Western	8 x 34	40 %
Niagara Solid	Decorative	Regular	Western	8 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	30 x 43	35 %
Nirmala UI	Swiss	Regular	Western	31 x 43	40 %
NSimSun	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
OCR A Extended	Modern	Regular	Western	19 x 33	40 %
Old English Text MT	Script	Regular	Western	12 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	8 x 37	40 %
Palace Script MT	Script	Regular	Western	7 x 30	40 %
Palatino Linotype	Roman	Regular	Baltic	14 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 43	40 %
Palatino Linotype	Roman	Regular	Cyrillic	14 x 43	40 %
Palatino Linotype	Roman	Regular	Greek	14 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 43	40 %
Palatino Linotype	Roman	Regular	Vietnamese	14 x 43	40 %
Palatino Linotype	Roman	Regular	Western	14 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 32	40 %
Papyrus	Script	Regular	Western	13 x 50	40 %
Parchment	Script	Regular	Western	6 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 38	30 %
Perpetua	Roman	Regular	Western	12 x 37	40 %
Playbill	Decorative	Regular	Western	8 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
PMingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
Poor Richard	Roman	Regular	Western	12 x 36	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	10 x 42	40 %
Proxy 1	Special	Regular	Arabic	20 x 39	40 %
Proxy 1	Special	Regular	Baltic	20 x 39	40 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 1	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 1	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 1	Special	Regular	Turkish	20 x 39	40 %
Proxy 1	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 2	Special	Regular	Arabic	20 x 39	40 %
Proxy 2	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 2	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 2	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 2	Special	Regular	Turkish	20 x 39	40 %
Proxy 2	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 3	Special	Regular	Arabic	20 x 39	40 %
Proxy 3	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 3	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 3	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 3	Special	Regular	Turkish	20 x 39	40 %
Proxy 3	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 4	Special	Regular	Arabic	20 x 39	40 %
Proxy 4	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 4	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 4	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 4	Special	Regular	Turkish	20 x 39	40 %
Proxy 4	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 5	Special	Regular	Arabic	20 x 39	40 %
Proxy 5	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 5	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 5	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 5	Special	Regular	Turkish	20 x 39	40 %
Proxy 5	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 6	Special	Regular	Arabic	20 x 39	40 %
Proxy 6	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 6	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 6	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 6	Special	Regular	Turkish	20 x 39	40 %
Proxy 6	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 7	Special	Regular	Arabic	20 x 39	40 %
Proxy 7	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %

Navigation

Proxy 7	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 7	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 7	Special	Regular	Turkish	20 x 39	40 %
Proxy 7	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 8	Special	Regular	Arabic	20 x 39	40 %
Proxy 8	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 8	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 8	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 8	Special	Regular	Turkish	20 x 39	40 %
Proxy 8	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 9	Special	Regular	Arabic	20 x 39	40 %
Proxy 9	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 9	Special	Regular	Cyrillic	20 x 39	40 %
Proxy 9	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Proxy 9	Special	Regular	Turkish	20 x 39	40 %
Proxy 9	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
Rage Italic	Script	Regular	Western	11 x 40	40 %
Ravie	Decorative	Regular	Western	22 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	11 x 38	40 %
Rockwell Extra Bold	Roman	Regular	Western	19 x 38	80 %
Rockwell	Roman	Regular	Western	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 37	40 %
RomanC	Special	Regular	Arabic	21 x 45	40 %
RomanC	Special	Regular	Baltic	21 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 45	40 %
RomanC	Special	Regular	Cyrillic	21 x 45	40 %
RomanC	Special	Regular	Greek	21 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 45	40 %
RomanC	Special	Regular	Turkish	21 x 45	40 %
RomanC	Special	Regular	Vietnamese	21 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 45	40 %
RomanD	Special	Regular	Arabic	20 x 46	40 %
RomanD	Special	Regular	Baltic	20 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 46	40 %
RomanD	Special	Regular	Cyrillic	20 x 46	40 %
RomanD	Special	Regular	Greek	20 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 46	40 %
RomanD	Special	Regular	Turkish	20 x 46	40 %
RomanD	Special	Regular	Vietnamese	20 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 46	40 %
RomanS	Special	Regular	Arabic	20 x 39	40 %
RomanS	Special	Regular	Baltic	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
RomanS	Special	Regular	Cyrillic	20 x 39	40 %
RomanS	Special	Regular	Greek	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
RomanS	Special	Regular	Turkish	20 x 39	40 %

Navigation

RomanS	Special	Regular	Vietnamese	20 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 39	40 %
RomanT	Special	Regular	Arabic	22 x 45	40 %
RomanT	Special	Regular	Baltic	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
RomanT	Special	Regular	Cyrillic	22 x 45	40 %
RomanT	Special	Regular	Greek	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
RomanT	Special	Regular	Turkish	22 x 45	40 %
RomanT	Special	Regular	Vietnamese	22 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 45	40 %
Romantic	Special	Regular	Symbol	13 x 36	40 %
SansSerif	Special	Regular	Symbol	14 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 39	70 %
Script	Script		OEM/DOS	16 x 36	40 %
ScriptC	Special	Regular	Arabic	15 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 51	40 %
ScriptC	Special	Regular	Central European	15 x 51	40 %
ScriptC	Special	Regular	Cyrillic	15 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 51	40 %
ScriptC	Special	Regular	Hebrew	15 x 51	40 %
ScriptC	Special	Regular	Turkish	15 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 51	40 %
ScriptC	Special	Regular	Western	15 x 51	40 %
ScriptS	Special	Regular	Arabic	16 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 51	40 %
ScriptS	Special	Regular	Central European	16 x 51	40 %
ScriptS	Special	Regular	Cyrillic	16 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 51	40 %
ScriptS	Special	Regular	Hebrew	16 x 51	40 %
ScriptS	Special	Regular	Turkish	16 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 51	40 %
ScriptS	Special	Regular	Western	16 x 51	40 %
Segoe MDL2 Assets	Roman	Regular	Western	33 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 56	40 %
Segoe Print	Special	Regular	Central European	21 x 56	40 %
Segoe Print	Special	Regular	Cyrillic	21 x 56	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 56	40 %
Segoe Print	Special	Regular	Turkish	21 x 56	40 %
Segoe Print	Special	Regular	Western	21 x 56	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 51	40 %
Segoe Script	Script	Regular	Central European	22 x 51	40 %
Segoe Script	Script	Regular	Cyrillic	22 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 51	40 %
Segoe Script	Script	Regular	Turkish	22 x 51	40 %
Segoe Script	Script	Regular	Western	22 x 51	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Central European	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Cyrillic	20 x 43	90 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Turkish	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Vietnamese	20 x 43	90 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	20 x 43	90 %
Segoe UI Emoji	Swiss	Regular	Western	40 x 43	40 %
Segoe UI Historic	Swiss	Regular	Western	27 x 43	40 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Baltic	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Central European	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Greek	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Hebrew	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Vietnamese	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Western	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Baltic	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Central European	18 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Greek	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Hebrew	18 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Vietnamese	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Western	18 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Baltic	18 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Central European	18 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Greek	18 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Hebrew	18 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Vietnamese	18 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Western	18 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 43	40 %
Segoe UI	Swiss	Regular	Arabic	17 x 43	40 %
Segoe UI	Swiss	Regular	Baltic	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
Segoe UI	Swiss	Regular	Cyrillic	17 x 43	40 %
Segoe UI	Swiss	Regular	Greek	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
Segoe UI	Swiss	Regular	Turkish	17 x 43	40 %
Segoe UI	Swiss	Regular	Vietnamese	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
Showcard Gothic	Decorative	Regular	Western	18 x 40	40 %
Simplex	Special	Regular	Arabic	19 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 44	40 %
Simplex	Special	Regular	Central European	19 x 44	40 %
Simplex	Special	Regular	Cyrillic	19 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 44	40 %
Simplex	Special	Regular	Hebrew	19 x 44	40 %
Simplex	Special	Regular	Turkish	19 x 44	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 44	40 %
Simplex	Special	Regular	Western	19 x 44	40 %
SimSun	Special	Regular	CHINESE_GB2312	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 32	40 %
SimSun-ExtB	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
SimSun-ExtB	Modern	Regular	Western	16 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 46	40 %
Sitka Banner	Special	Regular	Central European	16 x 46	40 %
Sitka Banner	Special	Regular	Cyrillic	16 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 46	40 %

Navigation

Sitka Banner	Special	Regular	Turkish	16 x 46	40 %
Sitka Banner	Special	Regular	Vietnamese	16 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 46	40 %
Sitka Display	Special	Regular	Baltic	17 x 46	40 %
Sitka Display	Special	Regular	Central European	17 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 46	40 %
Sitka Display	Special	Regular	Greek	17 x 46	40 %
Sitka Display	Special	Regular	Turkish	17 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 46	40 %
Sitka Display	Special	Regular	Western	17 x 46	40 %
Sitka Heading	Special	Regular	Baltic	17 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 46	40 %
Sitka Heading	Special	Regular	Cyrillic	17 x 46	40 %
Sitka Heading	Special	Regular	Greek	17 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 46	40 %
Sitka Heading	Special	Regular	Vietnamese	17 x 46	40 %
Sitka Heading	Special	Regular	Western	17 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 47	40 %
Sitka Small	Special	Regular	Central European	21 x 47	40 %
Sitka Small	Special	Regular	Cyrillic	21 x 47	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 47	40 %
Sitka Small	Special	Regular	Turkish	21 x 47	40 %
Sitka Small	Special	Regular	Vietnamese	21 x 47	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	21 x 47	40 %
Sitka Subheading	Special	Regular	Baltic	18 x 46	40 %
Sitka Subheading	Special	Regular	Central European	18 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 46	40 %
Sitka Subheading	Special	Regular	Greek	18 x 46	40 %
Sitka Subheading	Special	Regular	Turkish	18 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 46	40 %
Sitka Subheading	Special	Regular	Western	18 x 46	40 %
Sitka Text	Special	Regular	Baltic	19 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 46	40 %
Sitka Text	Special	Regular	Cyrillic	19 x 46	40 %
Sitka Text	Special	Regular	Greek	19 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 46	40 %
Sitka Text	Special	Regular	Vietnamese	19 x 46	40 %
Sitka Text	Special	Regular	Western	19 x 46	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	1 x 3	40 %
Snap ITC	Decorative	Regular	Western	19 x 41	40 %
Stencil	Decorative	Regular	Western	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	30 %
Stylus BT	Swiss	Roman	Greek	14 x 39	30 %
Stylus BT	Swiss	Roman	Mac	14 x 39	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	30 %
Stylus BT	Swiss	Roman	Western	14 x 39	30 %
SuperFrench	Special	Regular	Symbol	13 x 32	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 39	40 %
Swis721 BdCnOul BT	Decorative	Bold Outline	Greek	13 x 39	40 %
Swis721 BdCnOul BT	Decorative	Bold Outline	Mac	13 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 39	40 %
Swis721 BdCnOul BT	Decorative	Bold Outline	Western	13 x 39	40 %
Swis721 BdOul BT	Decorative	Bold	Central European	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 38	40 %
Swis721 BdOul BT	Decorative	Bold	Mac	15 x 38	40 %

Navigation

Swis721 BdOul BT	Decorative	Bold	Turkish	15 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 38	40 %
Swis721 Blk BT	Swiss	Black	Central European	18 x 38	40 %
Swis721 Blk BT	Swiss	Black	Greek	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Swis721 Blk BT	Swiss	Black	Turkish	18 x 38	40 %
Swis721 Blk BT	Swiss	Black	Western	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 38	40 %
Swis721 BlkCn BT	Swiss	Black	Greek	13 x 38	40 %
Swis721 BlkCn BT	Swiss	Black	Mac	13 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 38	40 %
Swis721 BlkCn BT	Swiss	Black	Western	13 x 38	40 %
Swis721 BlkEx BT	Swiss	Black	Central European	23 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 38	40 %
Swis721 BlkEx BT	Swiss	Black	Mac	23 x 38	40 %
Swis721 BlkEx BT	Swiss	Black	Turkish	23 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 38	40 %
Swis721 BlkOul BT	Decorative	Black	Central European	18 x 38	40 %
Swis721 BlkOul BT	Decorative	Black	Greek	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	18 x 38	40 %
Swis721 BlkOul BT	Decorative	Black	Turkish	18 x 38	40 %
Swis721 BlkOul BT	Decorative	Black	Western	18 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 38	40 %
Swis721 BT	Swiss	Roman	Greek	14 x 38	40 %
Swis721 BT	Swiss	Roman	Mac	14 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 38	40 %
Swis721 BT	Swiss	Roman	Western	14 x 38	40 %
Swis721 Cn BT	Swiss	Roman	Central European	12 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 38	40 %
Swis721 Cn BT	Swiss	Roman	Mac	12 x 38	40 %
Swis721 Cn BT	Swiss	Roman	Turkish	12 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 38	40 %
Swis721 Ex BT	Swiss	Roman	Central European	17 x 38	40 %
Swis721 Ex BT	Swiss	Roman	Greek	17 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 38	40 %
Swis721 Ex BT	Swiss	Roman	Turkish	17 x 38	40 %
Swis721 Ex BT	Swiss	Roman	Western	17 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 38	40 %
Swis721 Lt BT	Swiss	Light	Greek	14 x 38	40 %
Swis721 Lt BT	Swiss	Light	Mac	14 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 38	40 %
Swis721 Lt BT	Swiss	Light	Western	14 x 38	40 %
Swis721 LtCn BT	Swiss	Light	Central European	11 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	11 x 38	40 %
Swis721 LtCn BT	Swiss	Light	Mac	11 x 38	40 %
Swis721 LtCn BT	Swiss	Light	Turkish	11 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	11 x 38	40 %
Swis721 LtEx BT	Swiss	Light	Central European	16 x 38	40 %
Swis721 LtEx BT	Swiss	Light	Greek	16 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 38	40 %
Swis721 LtEx BT	Swiss	Light	Turkish	16 x 38	40 %
Swis721 LtEx BT	Swiss	Light	Western	16 x 38	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	24 x 37	40 %
Syastro	Special	Regular	Baltic	24 x 37	40 %
Syastro	Special	Regular	Central European	24 x 37	40 %

Navigation

[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	24 x 37	40 %
Syastro	Special	Regular	Greek	24 x 37	40 %
Syastro	Special	Regular	Hebrew	24 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	24 x 37	40 %
Syastro	Special	Regular	Vietnamese	24 x 37	40 %
Syastro	Special	Regular	Western	24 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 42	40 %
Sylfaen	Roman	Regular	Central European	13 x 42	40 %
Sylfaen	Roman	Regular	Cyrillic	13 x 42	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 42	40 %
Sylfaen	Roman	Regular	Turkish	13 x 42	40 %
Sylfaen	Roman	Regular	Western	13 x 42	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	28 x 91	40 %
Symap	Special	Regular	Baltic	28 x 91	40 %
Symap	Special	Regular	Central European	28 x 91	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	28 x 91	40 %
Symap	Special	Regular	Greek	28 x 91	40 %
Symap	Special	Regular	Hebrew	28 x 91	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	28 x 91	40 %
Symap	Special	Regular	Vietnamese	28 x 91	40 %
Symap	Special	Regular	Western	28 x 91	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	26 x 98	40 %
Symath	Special	Regular	Baltic	26 x 98	40 %
Symath	Special	Regular	Central European	26 x 98	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	26 x 98	40 %
Symath	Special	Regular	Greek	26 x 98	40 %
Symath	Special	Regular	Hebrew	26 x 98	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	26 x 98	40 %
Symath	Special	Regular	Vietnamese	26 x 98	40 %
Symath	Special	Regular	Western	26 x 98	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 39	40 %
Symeteo	Special	Regular	Arabic	17 x 45	40 %
Symeteo	Special	Regular	Baltic	17 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 45	40 %
Symeteo	Special	Regular	Cyrillic	17 x 45	40 %
Symeteo	Special	Regular	Greek	17 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 45	40 %
Symeteo	Special	Regular	Turkish	17 x 45	40 %
Symeteo	Special	Regular	Vietnamese	17 x 45	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 45	40 %
Symusic	Special	Regular	Arabic	23 x 69	40 %
Symusic	Special	Regular	Baltic	23 x 69	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 69	40 %
Symusic	Special	Regular	Cyrillic	23 x 69	40 %
Symusic	Special	Regular	Greek	23 x 69	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 69	40 %
Symusic	Special	Regular	Turkish	23 x 69	40 %
Symusic	Special	Regular	Vietnamese	23 x 69	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	23 x 69	40 %
System	Swiss		Western	7 x 16	70 %
Tahoma	Swiss	Regular	Arabic	14 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	40 %
Tahoma	Swiss	Regular	Central European	14 x 39	40 %
Tahoma	Swiss	Regular	Cyrillic	14 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	40 %

Navigation

Tahoma	Swiss	Regular	Hebrew	14 x 39	40 %
Tahoma	Swiss	Regular	Thai	14 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	14 x 39	40 %
Tahoma	Swiss	Regular	Vietnamese	14 x 39	40 %
Tahoma	Swiss	Regular	Western	14 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 34	40 %
TechnicBold	Special	Regular	Symbol	15 x 35	40 %
TechnicLite	Special	Regular	Symbol	15 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 42	40 %
Terminal	Modern		OEM/DOS	8 x 12	40 %
Times New Roman	Roman	Regular	Arabic	13 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 35	40 %
Times New Roman	Roman	Regular	Central European	13 x 35	40 %
Times New Roman	Roman	Regular	Cyrillic	13 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 35	40 %
Times New Roman	Roman	Regular	Hebrew	13 x 35	40 %
Times New Roman	Roman	Regular	Turkish	13 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 35	40 %
Times New Roman	Roman	Regular	Western	13 x 35	40 %
Trebuchet MS	Swiss	Regular	Baltic	15 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Cyrillic	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Greek	15 x 37	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Western	15 x 37	40 %
Tw Cen MT Condensed Extra Bold	Swiss	Regular	Central European	12 x 35	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	12 x 35	40 %
Tw Cen MT Condensed	Swiss	Regular	Central European	10 x 34	40 %
Tw Cen MT Condensed	Swiss	Regular	Western	10 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	13 x 35	40 %
Tw Cen MT	Swiss	Regular	Western	13 x 35	40 %
Txt	Special	Regular	Arabic	22 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 40	40 %
Txt	Special	Regular	Central European	22 x 40	40 %
Txt	Special	Regular	Cyrillic	22 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 40	40 %
Txt	Special	Regular	Hebrew	22 x 40	40 %
Txt	Special	Regular	Turkish	22 x 40	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	22 x 40	40 %
Txt	Special	Regular	Western	22 x 40	40 %
UniversalMath1 BT	Roman	Regular	Symbol	15 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
Verdana	Swiss	Regular	Central European	16 x 39	40 %
Verdana	Swiss	Regular	Cyrillic	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
Verdana	Swiss	Regular	Turkish	16 x 39	40 %
Verdana	Swiss	Regular	Vietnamese	16 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	16 x 39	40 %
Viner Hand ITC	Script	Regular	Western	15 x 52	40 %
Vineta BT	Decorative	Regular	Central European	25 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 43	40 %
Vineta BT	Decorative	Regular	Mac	25 x 43	40 %
Vineta BT	Decorative	Regular	Turkish	25 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 43	40 %
Vivaldi	Script	Italic	Western	9 x 38	40 %

Navigation

Vladimir Script	Script	Regular	Western	10 x 39	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 32	40 %
Wide Latin	Roman	Regular	Western	26 x 39	40 %
Wingdings 2	Roman	Regular	Symbol	27 x 34	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	25 x 36	40 %
Wingdings	Special	Regular	Symbol	28 x 36	40 %
Yu Gothic Light	Swiss	Regular	Baltic	31 x 41	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Cyrillic	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Greek	31 x 41	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Turkish	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Western	31 x 41	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	50 %
Yu Gothic Medium	Swiss	Regular	Central European	31 x 41	50 %
Yu Gothic Medium	Swiss	Regular	Cyrillic	31 x 41	50 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	50 %
Yu Gothic Medium	Swiss	Regular	Japanese	31 x 41	50 %
Yu Gothic Medium	Swiss	Regular	Turkish	31 x 41	50 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	50 %
Yu Gothic UI Light	Swiss	Regular	Baltic	17 x 43	30 %
Yu Gothic UI Light	Swiss	Regular	Central European	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
Yu Gothic UI Light	Swiss	Regular	Greek	17 x 43	30 %
Yu Gothic UI Light	Swiss	Regular	Japanese	17 x 43	30 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	30 %
Yu Gothic UI Light	Swiss	Regular	Western	17 x 43	30 %
Yu Gothic UI Semibold	Swiss	Regular	Baltic	19 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	60 %
Yu Gothic UI Semibold	Swiss	Regular	Cyrillic	19 x 43	60 %
Yu Gothic UI Semibold	Swiss	Regular	Greek	19 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	19 x 43	60 %
Yu Gothic UI Semibold	Swiss	Regular	Turkish	19 x 43	60 %
Yu Gothic UI Semibold	Swiss	Regular	Western	19 x 43	60 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	35 %
Yu Gothic UI Semilight	Swiss	Regular	Central European	17 x 43	35 %
Yu Gothic UI Semilight	Swiss	Regular	Cyrillic	17 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	35 %
Yu Gothic UI Semilight	Swiss	Regular	Japanese	17 x 43	35 %
Yu Gothic UI Semilight	Swiss	Regular	Turkish	17 x 43	35 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	35 %
Yu Gothic UI	Swiss	Regular	Baltic	17 x 43	40 %
Yu Gothic UI	Swiss	Regular	Central European	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
Yu Gothic UI	Swiss	Regular	Greek	17 x 43	40 %
Yu Gothic UI	Swiss	Regular	Japanese	17 x 43	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	17 x 43	40 %
Yu Gothic UI	Swiss	Regular	Western	17 x 43	40 %
Yu Gothic	Swiss	Regular	Baltic	31 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	40 %
Yu Gothic	Swiss	Regular	Cyrillic	31 x 41	40 %
Yu Gothic	Swiss	Regular	Greek	31 x 41	40 %
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	31 x 41	40 %
Yu Gothic	Swiss	Regular	Turkish	31 x 41	40 %
Yu Gothic	Swiss	Regular	Western	31 x 41	40 %

Navigation

Navigation

Windows Audio

Device	Identifier	Device Description
midi-out.0	0001 001B	Microsoft GS Wavetable Synth
mixer.0	0001 0068	Microphone (Realtek High Defini
mixer.1	0001 0068	Microphone (WO Mic Device)
mixer.2	0001 0068	Krisp Microphone (Krisp)
wave-in.0	0001 0065	Microphone (WO Mic Device)
wave-in.1	0001 0065	Microphone (Realtek High Defini
wave-in.2	0001 0065	Krisp Microphone (Krisp)

PCI / PnP Audio

Device Description	Type
Realtek ALC269 @ Intel Panther Point PCH - High Definition Audio Controller [C1]	PCI

HD Audio

[Intel Panther Point PCH - High Definition Audio Controller [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - High Definition Audio Controller [C1]
Device Description (Windows)	High Definition Audio Controller
Bus Type	PCI
Bus / Device / Function	0 / 27 / 0
Device ID	8086-1E20
Subsystem ID	10CF-176C
Revision	04
Hardware ID	PCI\VEN_8086&DEV_1E20&SUBSYS_176C10CF&REV_04

Device Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Realtek ALC269]

Device Properties:

Device Description	Realtek ALC269
Device Description (Windows)	Realtek High Definition Audio
Device Type	Audio
Bus Type	HDAUDIO
Device ID	10EC-0269
Subsystem ID	10CF-9000

Revision	1001
Hardware ID	HDAUDIO\FUNC_01&VEN_10EC&DEV_0269&SUBSYS_10CF9000&REV_1001

Navigation

Device Manufacturer:

Company Name	Realtek Semiconductor Corp.
Product Information	https://www.realtek.com/products
Driver Download	https://www.realtek.com/downloads
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Audio Codecs

[Fraunhofer IIS MPEG Layer-3 Codec (decode only)]

ACM Driver Properties:

Driver Description	Fraunhofer IIS MPEG Layer-3 Codec (decode only)
Copyright Notice	Copyright © 1996-1999 Fraunhofer Institut Integrierte Schaltungen IIS
Driver Features	decoder only version
Driver Version	1.09

[Microsoft ADPCM CODEC]

ACM Driver Properties:

Driver Description	Microsoft ADPCM CODEC
Copyright Notice	Copyright (C) 1992-1996 Microsoft Corporation
Driver Features	Compresses and decompresses Microsoft ADPCM audio data.
Driver Version	4.00

[Microsoft CCITT G.711 A-Law and u-Law CODEC]

ACM Driver Properties:

Driver Description	Microsoft CCITT G.711 A-Law and u-Law CODEC
Copyright Notice	Copyright (c) 1993-1996 Microsoft Corporation
Driver Features	Compresses and decompresses CCITT G.711 A-Law and u-Law audio data.
Driver Version	4.00

[Microsoft GSM 6.10 Audio CODEC]

ACM Driver Properties:

Driver Description	Microsoft GSM 6.10 Audio CODEC
Copyright Notice	Copyright (C) 1993-1996 Microsoft Corporation
Driver Features	Compresses and decompresses audio data conforming to the ETSI-GSM (European Telecommunications Standards Institute-Groupe Special Mobile) recommendation 6.10.
Driver Version	4.00

[Microsoft IMA ADPCM CODEC]

ACM Driver Properties:

Driver Description	Microsoft IMA ADPCM CODEC
Copyright Notice	Copyright (C) 1992-1996 Microsoft Corporation
Driver Features	Compresses and decompresses IMA ADPCM audio data.
Driver Version	4.00

[Microsoft PCM Converter]

Navigation

ACM Driver Properties:

Driver Description	Microsoft PCM Converter
Copyright Notice	Copyright (C) 1992-1996 Microsoft Corporation
Driver Features	Converts frequency and bits per sample of PCM audio data.
Driver Version	5.00

Video Codecs

Driver	Version	Description
iccvid.dll	1.10.0.11	Cinepak® Codec
iyuv_32.dll	10.0.19041.1 (WinBuild.160101.0800)	Intel Indeo(R) Video YUV Codec
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
msvidc32.dll	10.0.19041.1 (WinBuild.160101.0800)	Microsoft Video 1 Compressor
msyuv.dll	10.0.19041.1 (WinBuild.160101.0800)	Microsoft UYVY Video Decompressor
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]

MCI

[AVIVideo]

MCI Device Properties:

Device	AVIVideo
Name	Video for Windows
Description	Video For Windows MCI driver
Type	Digital Video Device
Driver	mciavi32.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Play In Reverse	Yes
Can Record	No
Can Save Data	No
Can Freeze Data	No
Can Lock Data	No
Can Stretch Frame	Yes
Can Stretch Input	No
Can Test	Yes
Audio Capable	Yes
Video Capable	Yes
Still Image Capable	No

[CDAudio]

Navigation

MCI Device Properties:

Device	CDAudio
Name	CD Audio
Description	MCI driver for cdaudio devices
Type	CD Audio Device
Driver	mcicda.dll
Status	Enabled

MCI Device Features:

Compound Device	No
File Based Device	No
Can Eject	Yes
Can Play	Yes
Can Record	No
Can Save Data	No
Audio Capable	Yes
Video Capable	No

[MPEGVideo]

MCI Device Properties:

Device	MPEGVideo
Name	DirectShow
Description	DirectShow MCI Driver
Type	Digital Video Device
Driver	mciqtz32.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Play In Reverse	No
Can Record	No
Can Save Data	No
Can Freeze Data	No
Can Lock Data	No
Can Stretch Frame	Yes
Can Stretch Input	No
Can Test	Yes
Audio Capable	Yes
Video Capable	Yes
Still Image Capable	No

[Sequencer]

MCI Device Properties:

Device	Sequencer
Name	MIDI Sequencer
Description	MCI driver for MIDI sequencer
Type	Sequencer Device
Driver	mciseq.dll
Status	Enabled

Navigation

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Record	No
Can Save Data	No
Audio Capable	Yes
Video Capable	No

[WaveAudio]

MCI Device Properties:

Device	WaveAudio
Name	Sound
Description	MCI driver for waveform audio
Type	Waveform Audio Device
Driver	mciwave.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	No
Can Record	Yes
Can Save Data	Yes
Audio Capable	Yes
Video Capable	No

SAPI

SAPI Properties:

SAPI4 Version	-
SAPI5 Version	5.3.24603.0

Voice (SAPI5):

Name	Microsoft David Desktop - English (United States)
Voice Path	C:\WINDOWS\Speech_OneCore\Engines\TTS\en-US\M1033David
Age	Adult
Gender	Male
Language	English (United States)
Vendor	Microsoft
Version	11.0
DLL File	C:\Windows\SysWOW64\speech_onecore\engines\tts\MSTTSEngine_OneCore.dll (x86)
CLSID	{179F3D56-1B0B-42B2-A962-59B7EF59FE1B}

Voice (SAPI5):

Name	Microsoft Zira Desktop - English (United States)
Voice Path	C:\WINDOWS\Speech\Engines\TTS\en-US\M1033ZIR
Age	Adult
Gender	Female

Language	English (United States)
Vendor	Microsoft
Version	11.0
DLL File	C:\Windows\SysWOW64\speech\engines\tts\MSTTSEngine.dll (x86)
CLSID	{C64501F6-E6E6-451f-A150-25D0839BC510}

Navigation

Speech Recognizer (SAPI5):

Name	Microsoft Speech Recognizer 8.0 for Windows (English - US)
Description	Microsoft Speech Recognizer 8.0 for Windows (English - US)
FE Config Data File	C:\WINDOWS\Speech\Engines\SR\en-US\c1033dsk.fe
Language	English (United States); English
Speaking Style	Discrete;Continuous
Supported Locales	English (United States); English (Canada); English (Philippines); English
Vendor	Microsoft
Version	8.0
DLL File	C:\WINDOWS\System32\Speech\Engines\SR\spsreng.dll (x64)
CLSID	{DAC9F469-0C67-4643-9258-87EC128C5941}
RecoExtension	{4F4DB904-CA35-4A3A-90AF-C9D8BE7532AC}

Windows Storage

[P3-128]

Device Properties:

Driver Description	P3-128
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	disk.inf
INF Section	disk_install.NT

[TSSTcorp CDDVDW SH-216DB]

Device Properties:

Driver Description	TSSTcorp CDDVDW SH-216DB
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	cdrom.inf
INF Section	cdrom_install

[Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem44.inf
INF Section	Intel_msahci_Inst

Device Resources:

IRQ	65536
Memory	F7C16000-F7C167FF
Port	F060-F07F
Port	F080-F083
Port	F090-F097
Port	F0A0-F0A3
Port	F0B0-F0B7

[Microsoft Storage Spaces Controller]

Device Properties:

Driver Description	Microsoft Storage Spaces Controller
Driver Date	6/21/2006
Driver Version	10.0.19041.423
Driver Provider	Microsoft
INF File	spaceport.inf
INF Section	Spaceport_Install

Logical Drives

Drive	Drive Type	File System	Total Size	Used Space	Free Space	% Free	Volume Serial
[TRIAL VERSION]	Local Disk	NTFS	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
E:	Optical Drive						

Physical Drives

[Drive #1 - P3-128 (119 GB) C:]

Partition	Partition Type	Drive	Start Offset	Partition Length
#1 (Active)	NTFS	C: (Windows 10)	1 MB	121559 MB
#2	Unknown (Code: $27)		121561 MB	542 MB

Optical Drives

[E:\ TSSTcorp CDDVDW SH-216DB]

Optical Drive Properties:

Device Description	TSSTcorp CDDVDW SH-216DB
Serial Number	R96R6YBF100057
Firmware Revision	FU01
Buffer Size	768 KB
Manufacturer	Toshiba-Samsung
Device Type	DVD+RW/DVD-RW/DVD-RAM
Interface	SATA
Extra Features	M-Disc
Region Code	2
Remaining User Changes	4

Remaining Vendor Changes	4

Navigation

Writing Speeds:

DVD+R9 Dual Layer	8x
DVD+R	16x
DVD+RW	8x
DVD-R9 Dual Layer	8x
DVD-R	16x
DVD-RW	6x
DVD-RAM	5x
CD-R	48x
CD-RW	24x

Reading Speeds:

DVD-ROM	16x
CD-ROM	48x

Supported Disk Types:

BD-ROM	Not Supported
BD-R	Not Supported
BD-RE	Not Supported
HD DVD-ROM	Not Supported
HD DVD-R Dual Layer	Not Supported
HD DVD-RW Dual Layer	Not Supported
HD DVD-R	Not Supported
HD DVD-RW	Not Supported
HD DVD-RAM	Not Supported
DVD-ROM	Read
DVD+R9 Dual Layer	Read + Write
DVD+RW9 Dual Layer	Not Supported
DVD+R	Read + Write
DVD+RW	Read + Write
DVD-R9 Dual Layer	Read + Write
DVD-RW9 Dual Layer	Not Supported
DVD-R	Read + Write
DVD-RW	Read + Write
DVD-RAM	Read + Write
CD-ROM	Read
CD-R	Read + Write
CD-RW	Read + Write

Optical Drive Features:

AACS	Not Supported
BD CPS	Not Supported
Buffer Underrun Protection	Supported
C2 Error Pointers	Supported
CD+G	Supported
CD-Text	Supported
DVD-Download Disc Recording	Not Supported
Hybrid Disc	Not Supported
JustLink	Supported
CPRM	Supported
CSS	Supported
LabelFlash	Not Supported
Layer-Jump Recording	Not Supported

Navigation

LightScribe	Not Supported
Mount Rainier	Not Supported
OSSC	Not Supported
Qflix Recording	Not Supported
SecurDisc	Not Supported
SMART	Not Supported
VCPS	Not Supported

Device Manufacturer:

Company Name	Toshiba Samsung Storage Technology
Product Information	http://www.tsstorage.com/tsst/index_e.html
Firmware Download	http://www.samsungodd.com/eng/LiveUpdate/LiveUpdate.asp
Driver Update	http://www.aida64.com/goto/?p=drvupdates

ASPI

Host	ID	LUN	Device Type	Vendor	Model	Rev	Extra Information
00	00	00	Disk Drive	P3-128			
00	00	00	Optical Drive	TSSTcorp	CDDVDW SH-216DB	FU01	
00	07	00	Host Adapter	storahci			

ATA

[P3-128 (088101897561)]

ATA Device Properties:

Model ID	P3-128
Serial Number	088101897561
Revision	H180806
World Wide Name	5-000000-000000000
Device Type	SATA-III
Parameters	248085 cylinders, 16 heads, 63 sectors per track, 512 bytes per sector
LBA Sectors	250069680
Physical / Logical Sector Size	512 bytes / 512 bytes
Multiple Sectors	16
Max. PIO Transfer Mode	PIO 4
Max. MWDMA Transfer Mode	MWDMA 2
Max. UDMA Transfer Mode	UDMA 6
Active UDMA Transfer Mode	UDMA 5
Unformatted Capacity	122104 MB
Form Factor	2.5"
Rotational Speed	SSD
ATA Standard	ACS-2

ATA Device Features:

48-bit LBA	Supported, Enabled
Automatic Acoustic Management (AAM)	Not Supported
Device Configuration Overlay (DCO)	Not Supported
DMA Setup Auto-Activate	Supported, Disabled
Free-Fall Control	Not Supported

Navigation

General Purpose Logging (GPL)	Supported, Enabled
Hardware Feature Control	Not Supported
Host Protected Area (HPA)	Not Supported
HPA Security Extensions	Not Supported
Hybrid Information Feature	Not Supported
In-Order Data Delivery	Not Supported
Native Command Queuing (NCQ)	Supported
NCQ Autosense	Not Supported
NCQ Priority Information	Not Supported
NCQ Queue Management Command	Not Supported
NCQ Streaming	Not Supported
Phy Event Counters	Supported
Read Look-Ahead	Supported, Enabled
Release Interrupt	Not Supported
Security Mode	Supported, Disabled
Sense Data Reporting (SDR)	Not Supported
Service Interrupt	Not Supported
SMART	Supported, Enabled
SMART Error Logging	Supported, Enabled
SMART Self-Test	Not Supported
Software Settings Preservation (SSP)	Supported, Enabled
Streaming	Not Supported
Tagged Command Queuing (TCQ)	Not Supported
Write Cache	Supported, Enabled
Write-Read-Verify	Not Supported

SSD Features:

Data Set Management	Supported
Deterministic Read After TRIM	Supported
TRIM Command	Supported

Power Management Features:

Advanced Power Management	Not Supported
Automatic Partial to Slumber Transitions (APST)	Disabled
Device Initiated Interface Power Management (DIPM)	Not Supported
Device Sleep (DEVSLP)	Not Supported
Extended Power Conditions (EPC)	Not Supported
Host Initiated Interface Power Management (HIPM)	Not Supported
IDLE IMMEDIATE With UNLOAD FEATURE	Not Supported
Link Power State Device Sleep	Not Supported
Power Management	Supported, Enabled
Power-Up In Standby (PUIS)	Not Supported

ATA Commands:

DEVICE RESET	Not Supported
DOWNLOAD MICROCODE	Supported, Enabled
FLUSH CACHE	Supported, Enabled
FLUSH CACHE EXT	Supported, Enabled
NOP	Supported, Enabled
READ BUFFER	Not Supported
WRITE BUFFER	Not Supported

SMART

Navigation

[P3-128 (088101897561)]

ID	Attribute Description	Threshold	Value	Worst	Data	Status
09	Power-On Time Count	0	100	100	6391	OK: Always passes
0C	Power Cycle Count	0	100	100	1680	OK: Always passes
A7	<vendor-specific>	0	100	100	0	OK: Always passes
A8	<vendor-specific>	0	100	100	4	OK: Always passes
A9	<vendor-specific>	10	97	97	2621450	OK: Value is normal
AB	<vendor-specific>	0	0	0	0	OK: Always passes
AC	<vendor-specific>	0	0	0	0	OK: Always passes
AD	<vendor-specific>	0	200	200	755927810237	OK: Always passes
AF	<vendor-specific>	10	100	100	0	OK: Value is normal
B4	<vendor-specific>	0	100	100	1656	OK: Always passes
BB	Reported Uncorrectable Errors	0	100	0	0	OK: Always passes
C0	Power-Off Retract Count	0	100	100	664	OK: Always passes
C2	Temperature	0	30	30	50, 10, 30	OK: Always passes
CE	Flying Height	0	200	200	176	OK: Always passes
CF	Spin High Current	0	200	200	207	OK: Always passes
D0	Spin Buzz	0	200	200	189	OK: Always passes
D1	Offline Seek Performance	0	200	200	331	OK: Always passes
D2	Ramp Load Value	0	200	200	6949	OK: Always passes
D3	Vibration During Write	0	200	200	4938	OK: Always passes
E7	Temperature	5	88	88	12	OK: Value is normal
F1	Total Host Writes	0	100	100	16593124422	OK: Always passes
F2	Total Host Reads	0	100	100	25141037972	OK: Always passes
F5	<vendor-specific>	0	100	100	0	OK: Always passes

Windows Network

[Bluetooth Personal Area Network Device]

Network Adapter Properties:

Network Adapter	Bluetooth Personal Area Network Device
Interface Type	Bluetooth Ethernet
Hardware Address	00-1A-7D-DA-71-11
Connection Name	Bluetooth Network Connection
Connection Speed	3 Mbps
MTU	1500 bytes
Bytes Received	0
Bytes Sent	0

[Realtek PCIe GbE Family Controller]

Network Adapter Properties:

Network Adapter	Realtek PCIe GbE Family Controller
Interface Type	Ethernet
Hardware Address	F8-0F-41-B1-FA-FB
Connection Name	Ethernet
Connection Speed	1 Gbps
MTU	1500 bytes
DHCP Lease Obtained	9/12/2020 8:48:15 PM

DHCP Lease Expires	9/13/2020 8:48:15 PM
Bytes Received	407845636 (389.0 MB)
Bytes Sent	40925430 (39.0 MB)

Navigation

Network Adapter Addresses:

IP / Subnet Mask	[TRIAL VERSION]
Gateway	[TRIAL VERSION]
DHCP	[TRIAL VERSION]
DNS	[TRIAL VERSION]
DNS	[TRIAL VERSION]

Network Adapter Manufacturer:

Company Name	Realtek Semiconductor Corp.
Product Information	https://www.realtek.com/products
Driver Download	https://www.realtek.com/downloads
Driver Update	http://www.aida64.com/goto/?p=drvupdates

PCI / PnP Network

Device Description	Type
Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter (PHY: Realtek RTL8211/8212)	PCI

Internet

Internet Settings:

Start Page	http://go.microsoft.com/fwlink/p/?LinkId=255141
Search Page	http://go.microsoft.com/fwlink/?LinkId=54896
Local Page	%11%\blank.htm
Download Folder	

Current Proxy:

Proxy Status	Disabled

LAN Proxy:

Proxy Status	Disabled

Routes

Type	Net Destination	Netmask	Gateway	Metric	Interface
Active	0.0.0.0	0.0.0.0	192.168.1.1	25	192.168.1.3 (Realtek PCIe GbE Family Controller)
Active	127.0.0.0	255.0.0.0	127.0.0.1	331	127.0.0.1 (Software Loopback Interface 1)
Active	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	331	[TRIAL VERSION]
Active	127.255.255.255	255.255.255.255	127.0.0.1	331	127.0.0.1 (Software Loopback Interface 1)
Active	192.168.1.0	255.255.255.0	192.168.1.3	281	192.168.1.3 (Realtek PCIe GbE Family Controller)
Active	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	281	[TRIAL VERSION]
Active	192.168.1.255	255.255.255.255	192.168.1.3	281	192.168.1.3 (Realtek PCIe GbE Family Controller)
Active	224.0.0.0	240.0.0.0	127.0.0.1	331	127.0.0.1 (Software Loopback Interface 1)
Active	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	281	[TRIAL VERSION]

Active	255.255.255.255	255.255.255.255	127.0.0.1	331	127.0.0.1 (Software Loopback Interface 1)
Active	255.255.255.255	255.255.255.255	192.168.1.3	281	192.168.1.3 (Realtek PCIe GbE Family Controller)

Navigation

IE Cookie

Last Access	URL
2020-09-08 13:58:09	bebos@quantserve.com/
2020-09-08 13:58:09	bebos@rlcdn.com/
2020-09-09 01:27:42	bebos@live.com/
2020-09-09 01:27:42	bebos@login.live.com/
2020-09-09 01:27:53	bebos@bing.com/
2020-09-12 19:18:10	bebos@autodesk.com/
2020-09-12 19:18:10	bebos@demdex.net/

Browser History

Last Access	URL
2020-09-08 13:58:04	bebos@clic://logger/?msg=2020-09-08%2013%3A58%3A04.465%20%7C%20info%20%7C%20%5BWebUI%5D%20Locale%3A%20en_US
2020-09-08 13:58:08	bebos@https://autodesk.demdex.net/dest5.html?d_nsid=0
2020-09-08 13:58:12	[TRIAL VERSION]
2020-09-08 13:59:47	bebos@res://C:%5CUsers%5Cbebos%5CAppData%5CLocal%5CTemp%5Cjds6097296.tmp%5CJavaSetup8u261.exe/welcome.html
2020-09-08 14:00:52	bebos@res://C:%5CUsers%5Cbebos%5CAppData%5CLocal%5CTemp%5Cjds6097296.tmp%5CJavaSetup8u261.exe/progress.html
2020-09-08 14:02:09	[TRIAL VERSION]
2020-09-08 14:04:43	bebos@file:///C:/Users/bebos/Desktop/USER%20LOGIN%20.docx
2020-09-08 14:10:44	bebos@file:///C:/Program%20Files/SketchUp/SketchUp%202020/Resources/en-US/eula.html
2020-09-08 14:20:34	[TRIAL VERSION]
2020-09-08 14:23:04	bebos@https://oobe.adobe.com/?error=invalid_scope
2020-09-08 19:34:40	bebos@file:///C:/Windows10Upgrade/resources/ux/default.htm
2020-09-08 19:34:40	[TRIAL VERSION]
2020-09-08 20:30:43	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(1).png
2020-09-08 20:33:46	bebos@file:///C:/Users/bebos/Downloads/com.mojang.rar
2020-09-08 20:33:48	[TRIAL VERSION]
2020-09-08 20:33:52	bebos@file:///C:/Users/bebos/Downloads
2020-09-08 20:35:53	bebos@ms-gamingoverlay://startuptips/?AumId=Microsoft.MinecraftUWP_8wekyb3d8bbwe%21App&ProcessId=4780&WindowId=853286
2020-09-09 01:27:41	[TRIAL VERSION]
2020-09-09	bebos@https://login.live.com/oauth20_logout.srf?client_id=00000000480728C5&redirect_uri=https://login.live.com/oauth20_desktop.srf

01:27:41	
2020-09-09 01:29:25	Navigation bebos@microsoft-edge:https://www.bing.com/search?q=show%20desktop%20icons%20windows%2010%20site:microsoft.com&form=ED0032&ocid=SettingsHAQ-BingIA&mkt=en-US
2020-09-09 01:29:47	[TRIAL VERSION]
2020-09-09 03:40:59	bebos@file:///C:/Program%20Files/Autodesk/AutoCAD%202021/Sample/ActiveX/ExtAttr/Assembly%20Sample.dwg
2020-09-09 03:40:59	bebos@file:///C:/Program%20Files/Autodesk/AutoCAD%202021/Sample/Database%20Connectivity/Floor%20Plan%20Sample.dwg
2020-09-09 03:40:59	[TRIAL VERSION]
2020-09-09 19:58:52	bebos@ms-settings:windowsupdate
2020-09-09 20:06:24	bebos@ms-gamingoverlay://startuptips/?AumId=Microsoft.MinecraftUWP_8wekyb3d8bbwe%21App&ProcessId=944&WindowId=197952
2020-09-09 20:09:40	[TRIAL VERSION]
2020-09-09 20:10:37	bebos@ms-gamingoverlay://startuptips/?AumId=Microsoft.MinecraftUWP_8wekyb3d8bbwe%21App&ProcessId=10656&WindowId=1180590
2020-09-09 20:11:31	bebos@ms-settings:privacy-voiceactivation
2020-09-09 20:16:36	[TRIAL VERSION]
2020-09-09 20:16:39	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(4).png
2020-09-09 20:17:18	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(5).png
2020-09-09 20:17:26	[TRIAL VERSION]
2020-09-09 20:17:31	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(7).png
2020-09-09 20:17:37	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(8).png
2020-09-09 20:17:41	[TRIAL VERSION]
2020-09-09 20:17:44	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(10).png
2020-09-09 20:20:00	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(2).png
2020-09-09 20:41:54	[TRIAL VERSION]
2020-09-09 20:41:56	bebos@clic://logger/?msg=2020-09-09%2020%3A41%3A56.395%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-10 16:08:18	bebos@clic://logger/?msg=2020-09-10%2016%3A08%3A18.922%20%7C%20info%20%7C%20%5BWebUI%5D%20Locale%3A%20en_US
2020-09-10 16:08:20	[TRIAL VERSION]
2020-09-10 16:08:21	bebos@clic://logger/?msg=2020-09-10%2016%3A08%3A21.348%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-10 16:08:25	bebos@clic://logger/?msg=2020-09-10%2016%3A08%3A25.237%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-10 16:28:02	[TRIAL VERSION]
2020-09-10 16:28:04	bebos@clic://logger/?msg=2020-09-10%2016%3A28%3A04.310%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-10 16:30:41	bebos@file:///C:/Users/bebos/Downloads/06-01-cad-blocks-net-doors-plan.zip
2020-09-10 18:22:26	[TRIAL VERSION]
2020-09-10 18:22:31	bebos@clic://logger/?msg=2020-09-10%2018%3A22%3A31.732%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined

2020-09-10 18:58:40	bebos@file:///C:/Users/bebos/Desktop/118985809_321844912393449_6104630446604757132_n.jpg
2020-09-10 19:00:55	[TRIAL VERSION]
2020-09-10 19:01:33	bebos@clic://logger/?msg=2020-09-10%2019%3A01%3A33.731%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-10 19:09:49	bebos@file:///C:/Users/bebos/Downloads/hmmm.dwg
2020-09-10 19:18:47	[TRIAL VERSION]
2020-09-10 19:18:51	bebos@clic://logger/?msg=2020-09-10%2019%3A18%3A51.476%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-10 19:27:42	bebos@clic://logger/?msg=2020-09-10%2019%3A27%3A42.91%20%7C%20info%20%7C%20%5BWebUI%5D%20Locale%3A%20en_US
2020-09-10 19:27:44	[TRIAL VERSION]
2020-09-10 20:49:57	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(11).png
2020-09-10 20:52:58	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(12).png
2020-09-11 11:21:59	[TRIAL VERSION]
2020-09-11 11:30:54	bebos@clic://logger/?msg=2020-09-11%2011%3A30%3A54.971%20%7C%20info%20%7C%20%5BWebUI%5D%20Locale%3A%20en_US
2020-09-11 11:31:34	bebos@clic://logger/?msg=2020-09-11%2011%3A31%3A34.19%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-11 12:20:55	[TRIAL VERSION]
2020-09-11 12:21:17	bebos@clic://logger/?msg=2020-09-11%2012%3A21%3A16.922%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-11 12:36:52	bebos@file:///C:/Users/bebos/Downloads/Villa%20Project%20Sample.dwg
2020-09-11 19:36:36	[TRIAL VERSION]
2020-09-11 19:36:38	bebos@clic://logger/?msg=2020-09-11%2019%3A36%3A38.295%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-11 20:01:59	bebos@file:///C:/Users/bebos/Desktop/118985809_321844912393449_610463044664757132_n.jpg
2020-09-11 20:21:03	[TRIAL VERSION]
2020-09-12 11:28:41	bebos@clic://logger/?msg=2020-09-12%2011%3A28%3A41.975%20%7C%20info%20%7C%20%5BWebUI%5D%20Locale%3A%20en_US
2020-09-12 11:28:44	bebos@clic://logger/?msg=2020-09-12%2011%3A28%3A44.414%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-12 11:55:27	[TRIAL VERSION]
2020-09-12 13:18:37	bebos@ms-gamingoverlay://startuptips/?AumId=Microsoft.MinecraftUWP_8wekyb3d8bbwe%21App&ProcessId=1528&WindowId=394402
2020-09-12 13:30:32	bebos@ms-gamingoverlay://startuptips/?AumId=Microsoft.MinecraftUWP_8wekyb3d8bbwe%21App&ProcessId=12144&WindowId=460036
2020-09-12 13:30:43	[TRIAL VERSION]
2020-09-12 13:30:44	bebos@ms-gamingoverlay://startuptips/?AumId=Microsoft.MinecraftUWP_8wekyb3d8bbwe%21App&ProcessId=7524&WindowId=196936
2020-09-12 15:47:19	bebos@file:///C:/Users/bebos/Downloads/dancing-line_2.7.3-mod-M.apk
2020-09-12 16:01:10	[TRIAL VERSION]
2020-09-12 16:01:23	bebos@file:///C:/Users/bebos/AppData/Local/Packages/Microsoft.Microsoft3DViewer_8wekyb3d8bbwe/TempState/Assets/Bee.glb
2020-09-12	bebos@file:///C:/Users/bebos/Downloads/ipadian-10-1-premium-crack-2020-with-serial-number-full-vers-1599901706.zip

16:08:11	
2020-09-12 16:08:22	[TRIAL VERSION]
2020-09-12 16:08:28	bebos@file:///C:/Users/bebos/Downloads/ipadian-10-1-premium-crack-2020-with-serial-number-full-vers-1599901715.zip
2020-09-12 16:23:12	bebos@file:///C:/Users/bebos/Downloads/ipadian-10-1-premium-crack-2020-with-serial-number-full-vers-1599902615.zip
2020-09-12 16:23:45	[TRIAL VERSION]
2020-09-12 16:26:24	bebos@file:///C:/Users/bebos/Downloads/ipadian-10-1-premium-crack-2020-with-serial-number-full-vers-1599902703.zip
2020-09-12 16:26:27	bebos@windowsdefender://threat/
2020-09-12 17:10:44	[TRIAL VERSION]
2020-09-12 19:18:05	bebos@about:blank
2020-09-12 19:18:05	bebos@clic://logger/?msg=2020-09-12%2019%3A18%3A05.160%20%7C%20info%20%7C%20%5BWebUI%5D%20Locale%3A%20en_US
2020-09-12 19:18:09	[TRIAL VERSION]
2020-09-12 19:18:36	bebos@clic://logger/?msg=2020-09-12%2019%3A18%3A36.28%20%7C%20info%20%7C%20%5BWebUI%5D%20hubService.action%20Action%20invoked%3A%20ChooseCancel%2C%20params%3A%20undefined
2020-09-12 19:18:48	bebos@file:///C:/Users/bebos/Documents/fist%20house.dwg
2020-09-12 19:34:36	[TRIAL VERSION]
2020-09-12 19:35:22	bebos@file:///C:/Users/bebos/Pictures/Screenshots/Screenshot%20(15).png
2020-09-12 19:47:01	bebos@ms-screenclip:?source=QuickActions
2020-09-12 20:01:10	[TRIAL VERSION]
2020-09-12 21:05:03	bebos@file:///C:/Users/bebos/AppData/Local/Temp/rpt-1.htm
2020-09-12 21:05:12	bebos@file:///C:/Users/bebos/Desktop/Report

DirectX Files

Name	Version	Type	Language	Size	Date
amstream.dll	10.00.19041.0001	Final Retail	English	76800	12/7/2019 4:10:04 PM
bdaplgin.ax	10.00.19041.0001	Final Retail	English	76288	12/7/2019 4:10:04 PM
d2d1.dll	10.00.19041.0329	Final Retail	English	5371536	8/9/2020 11:58:22 AM
d3d10.dll	10.00.19041.0001	Final Retail	English	1041920	12/7/2019 4:09:28 PM
d3d10_1.dll	10.00.19041.0001	Final Retail	English	151040	12/7/2019 4:09:28 PM
d3d10_1core.dll	10.00.19041.0001	Final Retail	English	34304	12/7/2019 4:09:28 PM
d3d10core.dll	10.00.19041.0001	Final Retail	English	33792	12/7/2019 4:09:28 PM
d3d10level9.dll	10.00.19041.0001	Final Retail	English	325344	12/7/2019 4:09:18 PM
d3d10warp.dll	10.00.19041.0001	Final Retail	English	5998608	12/7/2019 4:09:18 PM
d3d11.dll	10.00.19041.0001	Final Retail	English	1963408	12/7/2019 4:09:18 PM
d3d12.dll	10.00.19041.0423	Final Retail	English	1596464	8/11/2020 1:29:04 PM
d3d8.dll	10.00.19041.0001	Final Retail	English	714752	12/7/2019 4:09:26 PM
d3d8thk.dll	10.00.19041.0488	Final Retail	English	12800	9/9/2020 7:54:22 PM
d3d9.dll	10.00.19041.0488	Final Retail	English	1617088	9/9/2020 7:54:22 PM
d3dim.dll	10.00.19041.0001	Final Retail	English	318976	12/7/2019 4:09:26 PM

Navigation

d3dim700.dll	10.00.19041.0001	Final Retail	English	388096	12/7/2019 4:09:26 PM
d3dramp.dll	10.00.19041.0001	Final Retail	English	595456	12/7/2019 4:09:26 PM
d3dxof.dll	10.00.19041.0001	Final Retail	English	56832	12/7/2019 4:09:26 PM
ddraw.dll	10.00.19041.0001	Final Retail	English	527360	12/7/2019 4:09:26 PM
ddrawex.dll	10.00.19041.0001	Final Retail	English	41472	12/7/2019 4:09:26 PM
devenum.dll	10.00.19041.0329	Final Retail	English	93952	8/9/2020 11:58:58 AM
dinput.dll	10.00.19041.0001	Final Retail	English	135680	12/7/2019 4:09:57 PM
dinput8.dll	10.00.19041.0001	Final Retail	English	171008	12/7/2019 4:09:57 PM
dmband.dll	10.00.19041.0001	Final Retail	English	33792	12/7/2019 4:09:57 PM
dmcompos.dll	10.00.19041.0001	Final Retail	English	74240	12/7/2019 4:09:57 PM
dmime.dll	10.00.19041.0001	Final Retail	English	198656	12/7/2019 4:09:57 PM
dmloader.dll	10.00.19041.0001	Final Retail	English	41472	12/7/2019 4:09:57 PM
dmscript.dll	10.00.19041.0001	Final Retail	English	97280	12/7/2019 4:09:57 PM
dmstyle.dll	10.00.19041.0001	Final Retail	English	117760	12/7/2019 4:09:57 PM
dmsynth.dll	10.00.19041.0001	Final Retail	English	112640	12/7/2019 4:09:57 PM
dmusic.dll	10.00.19041.0001	Final Retail	English	109056	12/7/2019 4:09:57 PM
dplaysvr.exe	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dplayx.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpmodemx.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpnaddr.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpnathlp.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:58 PM
dpnet.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpnhpast.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpnhupnp.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpnlobby.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dpnsvr.exe	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:10:00 PM
dpwsockx.dll	10.00.19041.0001	Final Retail	English	8192	12/7/2019 4:09:57 PM
dsdmo.dll	10.00.19041.0001	Final Retail	English	183808	12/7/2019 4:09:11 PM
dsound.dll	10.00.19041.0001	Final Retail	English	493056	12/7/2019 4:09:11 PM
dswave.dll	10.00.19041.0001	Final Retail	English	23040	12/7/2019 4:09:57 PM
dwrite.dll	10.00.19041.0388	Final Retail	English	2104320	8/9/2020 11:58:22 AM
dxdiagn.dll	10.00.19041.0488	Final Retail	English	457728	9/9/2020 7:54:40 PM
dxgi.dll	10.00.19041.0488	Final Retail	English	782968	9/9/2020 7:54:20 PM
dxtmsft.dll	11.00.19041.0001	Final Retail	English	396288	12/7/2019 4:10:02 PM
dxtrans.dll	11.00.19041.0329	Final Retail	English	267776	8/9/2020 11:58:54 AM
dxva2.dll	10.00.19041.0001	Final Retail	English	106384	12/7/2019 4:09:18 PM
encapi.dll	10.00.19041.0001	Final Retail	English	20992	12/7/2019 4:10:04 PM
gcdef.dll	10.00.19041.0001	Final Retail	English	124416	12/7/2019 4:09:57 PM
iac25_32.ax	2.00.0005.0053	Final Retail	English	197632	12/7/2019 4:10:00 PM
ir41_32.ax	10.00.19041.0001	Final Retail	English	9216	12/7/2019 4:10:00 PM
ir41_qc.dll	10.00.19041.0001	Final Retail	English	8704	12/7/2019 4:10:00 PM
ir41_qcx.dll	10.00.19041.0001	Final Retail	English	8704	12/7/2019 4:10:00 PM
ir50_32.dll	10.00.19041.0001	Final Retail	English	9216	12/7/2019 4:10:00 PM
ir50_qc.dll	10.00.19041.0001	Final Retail	English	9216	12/7/2019 4:10:00 PM
ir50_qcx.dll	10.00.19041.0001	Final Retail	English	9216	12/7/2019 4:10:00 PM
ivfsrc.ax	5.10.0002.0051	Final Retail	English	146944	12/7/2019 4:10:00 PM
joy.cpl	10.00.19041.0001	Final Retail	English	90624	12/7/2019 4:09:57 PM
ksproxy.ax	10.00.19041.0001	Final Retail	English	234496	12/7/2019 4:10:04 PM
kstvtune.ax	10.00.19041.0001	Final Retail	English	89600	12/7/2019 4:10:04 PM
ksuser.dll	10.00.19041.0001	Final Retail	English	20328	12/7/2019 4:09:11 PM
kswdmcap.ax	10.00.19041.0001	Final Retail	English	116224	12/7/2019 4:10:04 PM
ksxbar.ax	10.00.19041.0001	Final Retail	English	53248	12/7/2019 4:10:04 PM
mciqtz32.dll	10.00.19041.0001	Final Retail	English	38400	12/7/2019 4:10:04 PM
mfc40.dll	4.01.0000.6140	Final Retail	English	924944	12/7/2019 4:09:13 PM
mfc42.dll	6.06.8063.0000	Beta Retail	English	1171456	12/7/2019 4:09:13 PM

Microsoft.DirectX.AudioVideoPlayback.dll	5.04.0000.2904	Final Retail	English	53248	9/9/2020 3:26:13 AM
Microsoft.DirectX.Diagnostics.dll	5.04.0000.2904	Final Retail	English	12800	9/9/2020 3:26:14 AM
Microsoft.DirectX.Direct3D.dll	9.05.0132.0000	Final Retail	English	473600	9/9/2020 3:26:14 AM
Microsoft.DirectX.Direct3DX.dll	5.04.0000.3900	Final Retail	English	2676224	9/9/2020 3:26:10 AM
Microsoft.DirectX.Direct3DX.dll	9.04.0091.0000	Final Retail	English	2846720	9/9/2020 3:26:11 AM
Microsoft.DirectX.Direct3DX.dll	9.05.0132.0000	Final Retail	English	563712	9/9/2020 3:26:11 AM
Microsoft.DirectX.Direct3DX.dll	9.06.0168.0000	Final Retail	English	567296	9/9/2020 3:26:11 AM
Microsoft.DirectX.Direct3DX.dll	9.07.0239.0000	Final Retail	English	576000	9/9/2020 3:26:12 AM
Microsoft.DirectX.Direct3DX.dll	9.08.0299.0000	Final Retail	English	577024	9/9/2020 3:26:12 AM
Microsoft.DirectX.Direct3DX.dll	9.09.0376.0000	Final Retail	English	577536	9/9/2020 3:26:12 AM
Microsoft.DirectX.Direct3DX.dll	9.10.0455.0000	Final Retail	English	577536	9/9/2020 3:26:13 AM
Microsoft.DirectX.Direct3DX.dll	9.11.0519.0000	Final Retail	English	578560	9/9/2020 3:26:13 AM
Microsoft.DirectX.Direct3DX.dll	9.12.0589.0000	Final Retail	English	578560	9/9/2020 3:26:14 AM
Microsoft.DirectX.DirectDraw.dll	5.04.0000.2904	Final Retail	English	145920	9/9/2020 3:26:14 AM
Microsoft.DirectX.DirectInput.dll	5.04.0000.2904	Final Retail	English	159232	9/9/2020 3:26:14 AM
Microsoft.DirectX.DirectPlay.dll	5.04.0000.2904	Final Retail	English	364544	9/9/2020 3:26:14 AM
Microsoft.DirectX.DirectSound.dll	5.04.0000.2904	Final Retail	English	178176	9/9/2020 3:26:15 AM
Microsoft.DirectX.dll	5.04.0000.2904	Final Retail	English	223232	9/9/2020 3:26:13 AM
mpeg2data.ax	10.00.19041.0001	Final Retail	English	75776	12/7/2019 4:10:04 PM
mpg2splt.ax	10.00.19041.0329	Final Retail	English	204800	8/9/2020 11:58:59 AM
msdmo.dll	10.00.19041.0001	Final Retail	English	28896	12/7/2019 4:09:11 PM
msdvbnp.ax	10.00.19041.0001	Final Retail	English	66560	12/7/2019 4:10:04 PM
msvidctl.dll	6.05.19041.0329	Final Retail	English	2202624	8/9/2020 11:58:59 AM
msyuv.dll	10.00.19041.0001	Final Retail	English	23552	12/7/2019 4:10:04 PM
pid.dll	10.00.19041.0001	Final Retail	English	38400	12/7/2019 4:09:57 PM
psisdecd.dll	10.00.19041.0329	Final Retail	English	484352	8/9/2020 11:58:59 AM
psisrndr.ax	10.00.19041.0001	Final Retail	English	80384	12/7/2019 4:10:04 PM
qasf.dll	12.00.19041.0001	Final Retail	English	127488	12/7/2019 4:10:00 PM
qcap.dll	10.00.19041.0001	Final Retail	English	211968	12/7/2019 4:10:04 PM
qdv.dll	10.00.19041.0001	Final Retail	English	291328	12/7/2019 4:10:04 PM
qdvd.dll	10.00.19041.0329	Final Retail	English	549888	8/9/2020 11:58:58 AM
qedit.dll	10.00.19041.0329	Final Retail	English	556544	8/9/2020 11:58:59 AM
qedwipes.dll	10.00.19041.0001	Final Retail	English	2560	12/7/2019 4:10:05 PM
quartz.dll	10.00.19041.0329	Final Retail	English	1470976	8/9/2020 11:58:58 AM
vbisurf.ax	10.00.19041.0001	Final Retail	English	37888	12/7/2019 4:10:04 PM
vfwwdm32.dll	10.00.19041.0001	Final Retail	English	56832	12/7/2019 4:10:04 PM
wsock32.dll	10.00.19041.0001	Final Retail	English	16384	12/7/2019 4:09:15 PM

Navigation

DirectX Video

[Primary Display Driver]

DirectDraw Device Properties:

DirectDraw Driver Name	display
DirectDraw Driver Description	Primary Display Driver
Hardware Driver	igdumdim32.dll (10.18.10.5129)
Hardware Description	Intel(R) HD Graphics

Direct3D Device Properties:

Rendering Bit Depths	8, 16, 32
Z-Buffer Bit Depths	16, 24, 32
Multisample Anti-Aliasing Modes	MSAA 2x, MSAA 4x, MSAA 8x

Min Texture Size	1 x 1
Max Texture Size	8192 x 8192
Unified Shader Version	5.0
DirectX Hardware Support	DirectX v11.0

Direct3D Device Features:

Additive Texture Blending	Supported
AGP Texturing	Not Supported
Anisotropic Filtering	Supported
Automatic Mipmap Generation	Supported
Bilinear Filtering	Supported
Compute Shader	Supported
Cubic Environment Mapping	Supported
Cubic Filtering	Not Supported
Decal-Alpha Texture Blending	Supported
Decal Texture Blending	Supported
Directional Lights	Supported
DirectX Texture Compression	Not Supported
DirectX Volumetric Texture Compression	Not Supported
Dithering	Supported
Dot3 Texture Blending	Supported
Double-Precision Floating-Point	Supported
Driver Concurrent Creates	Supported
Driver Command Lists	Not Supported
Dynamic Textures	Supported
Edge Anti-Aliasing	Not Supported
Environmental Bump Mapping	Supported
Environmental Bump Mapping + Luminance	Supported
Factor Alpha Blending	Supported
Geometric Hidden-Surface Removal	Not Supported
Geometry Shader	Supported
Guard Band	Supported
Hardware Scene Rasterization	Supported
Hardware Transform & Lighting	Supported
Legacy Depth Bias	Supported
Map On Default Buffers	Supported
Mipmap LOD Bias Adjustments	Supported
Mipmapped Cube Textures	Supported
Mipmapped Volume Textures	Supported
Modulate-Alpha Texture Blending	Supported
Modulate Texture Blending	Supported
Non-Square Textures	Supported
N-Patches	Not Supported
Perspective Texture Correction	Supported
Point Lights	Supported
Point Sampling	Supported
Projective Textures	Supported
Quintic Bezier Curves & B-Splines	Not Supported
Range-Based Fog	Supported
Rectangular & Triangular Patches	Not Supported
Rendering In Windowed Mode	Supported
Runtime Shader Linking	Supported
Scissor Test	Supported
Slope-Scale Based Depth Bias	Supported
Specular Flat Shading	Supported

Navigation

Specular Gouraud Shading	Supported
Specular Phong Shading	Not Supported
Spherical Mapping	Supported
Spot Lights	Supported
Stencil Buffers	Supported
Sub-Pixel Accuracy	Supported
Subtractive Texture Blending	Supported
Table Fog	Supported
Texture Alpha Blending	Supported
Texture Clamping	Supported
Texture Mirroring	Supported
Texture Transparency	Supported
Texture Wrapping	Supported
Tiled Resources	Not Supported
Triangle Culling	Not Supported
Trilinear Filtering	Supported
Two-Sided Stencil Test	Supported
Vertex Alpha Blending	Supported
Vertex Fog	Supported
Vertex Tweening	Supported
Volume Textures	Supported
W-Based Fog	Supported
W-Buffering	Not Supported
Z-Based Fog	Supported
Z-Bias	Supported
Z-Test	Supported

Supported FourCC Codes:

AI44	Supported
AYUV	Supported
I420	Supported
IA44	Supported
IMC1	Supported
IMC2	Supported
IMC3	Supported
IMC4	Supported
IYUV	Supported
NV11	Supported
NV12	Supported
P208	Supported
UYVY	Supported
VYUY	Supported
YUY2	Supported
YV12	Supported
YVU9	Supported
YVYU	Supported

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

DirectX Sound

Navigation

[Primary Sound Driver]

DirectSound Device Properties:

Device Description	Primary Sound Driver
Driver Module	
Primary Buffers	0
Min / Max Secondary Buffers Sample Rate	0 / 0 Hz
Primary Buffers Sound Formats	None
Secondary Buffers Sound Formats	None
Total / Free Sound Buffers	0 / 0
Total / Free Static Sound Buffers	0 / 0
Total / Free Streaming Sound Buffers	0 / 0
Total / Free 3D Sound Buffers	0 / 0
Total / Free 3D Static Sound Buffers	0 / 0
Total / Free 3D Streaming Sound Buffers	0 / 0

DirectSound Device Features:

Certified Driver	No
Emulated Device	No
Precise Sample Rate	Not Supported
DirectSound3D	Not Supported
Creative EAX 1.0	Not Supported
Creative EAX 2.0	Not Supported
Creative EAX 3.0	Not Supported
Creative EAX 4.0	Not Supported
Creative EAX 5.0	Not Supported
I3DL2	Not Supported
Sensaura ZoomFX	Not Supported

Windows Devices

[Devices]

Audio inputs and outputs:

Krisp Microphone (Krisp)	10.0.19041.1
Microphone (Realtek High Definition Audio)	10.0.19041.1
Microphone (WO Mic Device)	10.0.19041.1

Bluetooth Radios:

CSR Bluetooth Radio	2.1.61.0

Computer:

ACPI x64-based PC	10.0.19041.1

Disk drives:

P3-128	10.0.19041.1

Display adapters:

Intel(R) HD Graphics	10.18.10.5129

Navigation

DVD/CD-ROM drives:

TSSTcorp CDDVDW SH-216DB	10.0.19041.1

Human Interface Devices:

Bluetooth Hands Free Device	2.1.52.0
Bluetooth Hands Free Device	2.1.52.0
Bluetooth Remote Control Device	2.1.51.0
HID-compliant consumer control device	10.0.19041.1
HID-compliant consumer control device	10.0.19041.1
HID-compliant consumer control device	10.0.19041.1
HID-compliant consumer control device	10.0.19041.1
HID-compliant device	10.0.19041.1
HID-compliant device	10.0.19041.1
HID-compliant device	10.0.19041.1
HID-compliant device	10.0.19041.1
HID-compliant device	10.0.19041.1
HID-compliant phone	10.0.19041.1
HID-compliant phone	10.0.19041.1
HID-compliant system controller	10.0.19041.1
HID-compliant vendor-defined device	10.0.19041.1
USB Input Device	10.0.19041.1
USB Input Device	10.0.19041.1
USB Input Device	10.0.19041.1

IDE ATA/ATAPI controllers:

Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02	9.3.0.1029

Keyboards:

HID Keyboard Device	10.0.19041.1

Mice and other pointing devices:

HID-compliant mouse	10.0.19041.1

Modems:

SAMSUNG Mobile USB Modem	2.16.15.0

Monitors:

Generic PnP Monitor	10.0.19041.488

Network adapters:

Bluetooth Personal Area Network Device	2.1.51.0
Microsoft Kernel Debug Network Adapter	10.0.19041.1
RAS Async Adapter	10.0.19041.1
Realtek PCIe GbE Family Controller	10.42.526.2020
WAN Miniport (IKEv2)	10.0.19041.1
WAN Miniport (IP)	10.0.19041.1
WAN Miniport (IPv6)	10.0.19041.1
WAN Miniport (L2TP)	10.0.19041.1
WAN Miniport (Network Monitor)	10.0.19041.1
WAN Miniport (PPPOE)	10.0.19041.1
WAN Miniport (PPTP)	10.0.19041.1
WAN Miniport (SSTP)	10.0.19041.1

Portable Devices:

SMJ320H	2.9.317.215

Navigation

Ports (COM & LPT):

Bluetooth SPP Driver (COM4)	2.1.51.0
Bluetooth SPP Driver (COM5)	2.1.51.0
Communications Port (COM1)	10.0.19041.1
Printer Port (LPT1)	10.0.19041.1

Print queues:

Fax	10.0.19041.1
Microsoft Print to PDF	10.0.19041.1
Microsoft XPS Document Writer	10.0.19041.1
OneNote for Windows 10	10.0.19041.1
Root Print Queue	10.0.19041.1
Send To OneNote 2016	10.0.19041.1

Processors:

Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	10.0.19041.1
Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	10.0.19041.1
Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	10.0.19041.1
Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	10.0.19041.1

SAMSUNG Android Phone:

SAMSUNG Android ADB Interface	2.16.15.0

Software devices:

Microsoft Device Association Root Enumerator	10.0.19041.1
Microsoft GS Wavetable Synth	10.0.19041.1
Microsoft Radio Device Enumeration Bus	10.0.19041.1
Microsoft RRAS Root Enumerator	10.0.19041.1

Sound, video and game controllers:

Bluetooth Hands-free Audio Device	2.1.60.0
Bluetooth Hands-free Audio Device	2.1.60.0
Bluetooth Stereo Audio	2.1.60.0
Bluetooth Stereo Audio	2.1.60.0
Bluetooth Stereo Audio	2.1.60.0
Krisp	0.8.3.0
Realtek High Definition Audio	6.0.8746.1
WO Mic Device	1.6.0.0

Storage controllers:

Microsoft Storage Spaces Controller	10.0.19041.423

Storage volumes:

Volume	10.0.19041.1
Volume	10.0.19041.1

System devices:

ACPI Fixed Feature Button	10.0.19041.1
ACPI Power Button	10.0.19041.1
Composite Bus Enumerator	10.0.19041.1
Direct memory access controller	10.0.19041.1
Fujitsu FUJ02E3 Device Driver	4.3.0.1
High Definition Audio Controller	10.0.19041.1
High Precision Event Timer	7.0.0.1011

Navigation

Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10	10.1.1.45
Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12	10.1.1.45
Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1E22	10.1.1.45
Intel(R) 82801 PCI Bridge - 244E	7.0.0.1011
Intel(R) B75 Express Chipset LPC Controller - 1E49	10.1.1.45
Intel(R) Management Engine Interface	11.0.5.1189
Legacy device	10.0.19041.1
Microsoft ACPI-Compliant System	10.0.19041.488
Microsoft Basic Display Driver	10.0.19041.1
Microsoft Basic Render Driver	10.0.19041.84
Microsoft Hyper-V Virtualization Infrastructure Driver	10.0.19041.423
Microsoft System Management BIOS Driver	10.0.19041.1
Microsoft Virtual Drive Enumerator	10.0.19041.1
Motherboard resources	10.0.19041.1
Motherboard resources	10.0.19041.1
Motherboard resources	10.0.19041.1
Motherboard resources	10.0.19041.1
Motherboard resources	10.0.19041.1
NDIS Virtual Network Adapter Enumerator	10.0.19041.1
Numeric data processor	10.0.19041.1
PCI Express Root Complex	10.0.19041.488
Plug and Play Software Device Enumerator	10.0.19041.1
Printer Port Logical Interface	10.0.19041.1
Programmable interrupt controller	10.0.19041.1
Remote Desktop Device Redirector Bus	10.0.19041.1
System board	10.0.19041.1
System board	10.0.19041.1
System CMOS/real time clock	10.0.19041.1
System timer	10.0.19041.1
UMBus Root Bus Enumerator	10.0.19041.1
Volume Manager	10.0.19041.1
Xeon(R) processor E3 - 1200 v2/3rd Gen Core processor DRAM Controller - 0150	10.1.1.45

Universal Serial Bus controllers:

CSR BlueCore Device	2.1.60.0
Generic USB Hub	10.0.19041.488
Generic USB Hub	10.0.19041.488
Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26	9.3.0.1030
Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D	9.3.0.1030
Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)	10.0.19041.488
SAMSUNG Mobile USB Composite Device	2.16.15.0
USB Composite Device	10.0.19041.488
USB Root Hub (USB 3.0)	10.0.19041.264
USB Root Hub	10.0.19041.1
USB Root Hub	10.0.19041.1

Unknown:

Unknown

[Audio inputs and outputs / Krisp Microphone (Krisp)]

Device Properties:

Driver Description	Krisp Microphone (Krisp)
Driver Date	12/6/2019
Driver Version	10.0.19041.1

Driver Provider	Microsoft
INF File	audioendpoint.inf
INF Section	NO_DRV
Hardware ID	MMDEVAPI\AudioEndpoints

Navigation

[Audio inputs and outputs / Microphone (Realtek High Definition Audio)]

Device Properties:

Driver Description	Microphone (Realtek High Definition Audio)
Driver Date	12/6/2019
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	audioendpoint.inf
INF Section	NO_DRV
Hardware ID	MMDEVAPI\AudioEndpoints

[Audio inputs and outputs / Microphone (WO Mic Device)]

Device Properties:

Driver Description	Microphone (WO Mic Device)
Driver Date	12/6/2019
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	audioendpoint.inf
INF Section	NO_DRV
Hardware ID	MMDEVAPI\AudioEndpoints

[Bluetooth Radios / CSR Bluetooth Radio]

Device Properties:

Driver Description	CSR Bluetooth Radio
Driver Date	2/27/2012
Driver Version	2.1.61.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem4.inf
INF Section	CsrBtPort_Device.NT
Hardware ID	{473a6b1d-3407-400e-b91a-f991c5a39dc3}\CsrBtPort
Location Information	CSRBCBUS Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Computer / ACPI x64-based PC]

Device Properties:

Driver Description	ACPI x64-based PC
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	hal.inf
INF Section	ACPI_AMD64_HAL
Hardware ID	acpiapic

[Disk drives / P3-128]

Navigation

Device Properties:

Driver Description	P3-128
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	disk.inf
INF Section	disk_install.NT
Hardware ID	SCSI\Disk__P3-128_____H180
Location Information	Bus Number 0, Target Id 0, LUN 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Display adapters / Intel(R) HD Graphics]

Device Properties:

Driver Description	Intel(R) HD Graphics
Driver Date	1/21/2020
Driver Version	10.18.10.5129
Driver Provider	Intel Corporation
INF File	oem51.inf
INF Section	iIVBD_w10
Hardware ID	PCI\VEN_8086&DEV_0152&SUBSYS_176D10CF&REV_09
Location Information	PCI bus 0, device 2, function 0
PCI Device	Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)

Device Resources:

IRQ	65536
Memory	000A0000-000BFFFF
Memory	E0000000-EFFFFFFF
Memory	F7800000-F7BFFFFF
Port	03B0-03BB
Port	03C0-03DF
Port	F000-F03F

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[DVD/CD-ROM drives / TSSTcorp CDDVDW SH-216DB]

Device Properties:

Driver Description	TSSTcorp CDDVDW SH-216DB
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	cdrom.inf
INF Section	cdrom_install
Hardware ID	SCSI\CdRomTSSTcorpCDDVDW_SH-216DB_FU01
Location Information	Bus Number 4, Target Id 0, LUN 0

Device Manufacturer:

Company Name	Toshiba Samsung Storage Technology
Product Information	http://www.tsstorage.com/tsst/index_e.html
Firmware Download	http://www.samsungodd.com/eng/LiveUpdate/LiveUpdate.asp
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Navigation

[Human Interface Devices / Bluetooth Hands Free Device]

Device Properties:

Driver Description	Bluetooth Hands Free Device
Driver Date	12/29/2011
Driver Version	2.1.52.0
Driver Provider	Cambridge Silicon Radio Limited.
INF File	oem29.inf
INF Section	csrhfgcc_DDI.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrHFGCC_111E
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / Bluetooth Hands Free Device]

Device Properties:

Driver Description	Bluetooth Hands Free Device
Driver Date	12/29/2011
Driver Version	2.1.52.0
Driver Provider	Cambridge Silicon Radio Limited.
INF File	oem29.inf
INF Section	csrhfgcc_DDI.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrHFGCC_111E
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / Bluetooth Remote Control Device]

Device Properties:

Driver Description	Bluetooth Remote Control Device
Driver Date	12/22/2011
Driver Version	2.1.51.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem23.inf
INF Section	csravrcp_DDI.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrAVRCP_110E
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant consumer control device]

Device Properties:

Driver Description	HID-compliant consumer control device

Navigation

Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	hidserv.inf
INF Section	HIDSystemConsumerDevice
Hardware ID	HID\VID_04D9&PID_1503&REV_0403&MI_01&Col02

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant consumer control device]

Device Properties:

Driver Description	HID-compliant consumer control device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	hidserv.inf
INF Section	HIDSystemConsumerDevice
Hardware ID	HID\hfgCcDevice&Col04

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant consumer control device]

Device Properties:

Driver Description	HID-compliant consumer control device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	hidserv.inf
INF Section	HIDSystemConsumerDevice
Hardware ID	HID\BthAvrcpDevice&Col01

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant consumer control device]

Device Properties:

Driver Description	HID-compliant consumer control device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	hidserv.inf
INF Section	HIDSystemConsumerDevice
Hardware ID	HID\hfgCcDevice&Col04

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant device]

Navigation

Device Properties:

Driver Description	HID-compliant device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\hfgCcDevice&Col02

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant device]

Device Properties:

Driver Description	HID-compliant device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\hfgCcDevice&Col03

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant device]

Device Properties:

Driver Description	HID-compliant device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\BthAvrcpDevice&Col03

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant device]

Device Properties:

Driver Description	HID-compliant device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\hfgCcDevice&Col02

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant device]

Navigation

Device Properties:

Driver Description	HID-compliant device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\hfgCcDevice&Col03

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant phone]

Device Properties:

Driver Description	HID-compliant phone
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\hfgCcDevice&Col01

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant phone]

Device Properties:

Driver Description	HID-compliant phone
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\hfgCcDevice&Col01

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / HID-compliant system controller]

Device Properties:

Driver Description	HID-compliant system controller
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\VID_04D9&PID_1503&REV_0403&MI_01&Col01

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

Navigation

[Human Interface Devices / HID-compliant vendor-defined device]

Device Properties:

Driver Description	HID-compliant vendor-defined device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Raw_Inst.NT
Hardware ID	HID\BthAvrcpDevice&Col02

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / USB Input Device]

Device Properties:

Driver Description	USB Input Device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Inst.NT
Hardware ID	USB\VID_04D9&PID_1503&REV_0403&MI_00
Location Information	0000.001a.0000.001.001.000.000.000.000

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / USB Input Device]

Device Properties:

Driver Description	USB Input Device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf
INF Section	HID_Inst.NT
Hardware ID	USB\VID_04D9&PID_1503&REV_0403&MI_01
Location Information	0000.001a.0000.001.001.000.000.000.000

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Human Interface Devices / USB Input Device]

Device Properties:

Driver Description	USB Input Device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	input.inf

INF Section	HID_Inst.NT
Hardware ID	USB\VID_093A&PID_2510&REV_0100
Location Information	Port_#0002.Hub_#0004

Navigation

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[IDE ATA/ATAPI controllers / Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem44.inf
INF Section	Intel_msahci_Inst
Hardware ID	PCI\VEN_8086&DEV_1E02&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 31, function 2
PCI Device	Intel Panther Point PCH - SATA AHCI Controller [C1]

Device Resources:

IRQ	65536
Memory	F7C16000-F7C167FF
Port	F060-F07F
Port	F080-F083
Port	F090-F097
Port	F0A0-F0A3
Port	F0B0-F0B7

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Keyboards / HID Keyboard Device]

Device Properties:

Driver Description	HID Keyboard Device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	keyboard.inf
INF Section	HID_Keyboard_Inst.NT
Hardware ID	HID\VID_04D9&PID_1503&REV_0403&MI_00

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Mice and other pointing devices / HID-compliant mouse]

Device Properties:

Driver Description	HID-compliant mouse

Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	msmouse.inf
INF Section	HID_Mouse_Inst.NT
Hardware ID	HID\VID_093A&PID_2510&REV_0100

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Modems / SAMSUNG Mobile USB Modem]

Device Properties:

Driver Description	SAMSUNG Mobile USB Modem
Driver Date	5/6/2020
Driver Version	2.16.15.0
Driver Provider	SAMSUNG Electronics Co., Ltd.
INF File	oem37.inf
INF Section	ssud.Install.NT
Hardware ID	USB\VID_04E8&PID_6860&REV_0400&Modem

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Monitors / Generic PnP Monitor]

Device Properties:

Driver Description	Generic PnP Monitor
Driver Date	6/21/2006
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	monitor.inf
INF Section	PnPMonitor.Install
Hardware ID	MONITOR\SAM06B7
Monitor	Samsung SyncMaster E1920/E1920X/EX1920/EX1920X (Analog)

Monitor Manufacturer:

Company Name	Samsung
Product Information	http://www.samsung.com/us/computer/monitors
Driver Download	http://www.samsung.com/us/support
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / Bluetooth Personal Area Network Device]

Device Properties:

Driver Description	Bluetooth Personal Area Network Device
Driver Date	12/22/2011
Driver Version	2.1.51.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem14.inf
INF Section	csrpan.ndi.NTamd64
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrPAN
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

Navigation

[Network adapters / Microsoft Kernel Debug Network Adapter]

Device Properties:

Driver Description	Microsoft Kernel Debug Network Adapter
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	kdnic.inf
INF Section	KdNic.ndi
Hardware ID	root\kdnic

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / RAS Async Adapter]

Device Properties:

Driver Description	RAS Async Adapter
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-AsyncMac
Hardware ID	SW\{eeab7790-c514-11d1-b42b-00805fc1270e}

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / Realtek PCIe GbE Family Controller]

Device Properties:

Driver Description	Realtek PCIe GbE Family Controller
Driver Date	5/26/2020
Driver Version	10.42.526.2020
Driver Provider	Realtek
INF File	oem12.inf
INF Section	RTL8168FS5WOLARPOffload.ndi.NT
Hardware ID	PCI\VEN_10EC&DEV_8168&SUBSYS_175A10CF&REV_07
Location Information	PCI bus 2, device 0, function 0
PCI Device	Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter

Device Resources:

IRQ	17
Memory	F0000000-F0003FFF
Memory	F0004000-F0004FFF
Port	E000-E0FF

Network Adapter Manufacturer:

Company Name	Realtek Semiconductor Corp.
Product Information	https://www.realtek.com/products
Driver Download	https://www.realtek.com/downloads

Driver Update	http://www.aida64.com/goto/?p=drvupdates

Navigation

[Network adapters / WAN Miniport (IKEv2)]

Device Properties:

Driver Description	WAN Miniport (IKEv2)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netavpna.inf
INF Section	Ndi-Mp-AgileVpn
Hardware ID	ms_agilevpnminiport

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (IP)]

Device Properties:

Driver Description	WAN Miniport (IP)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-Ip
Hardware ID	ms_ndiswanip

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (IPv6)]

Device Properties:

Driver Description	WAN Miniport (IPv6)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-Ipv6
Hardware ID	ms_ndiswanipv6

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (L2TP)]

Device Properties:

Driver Description	WAN Miniport (L2TP)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-L2tp
Hardware ID	ms_l2tpminiport

Navigation

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (Network Monitor)]

Device Properties:

Driver Description	WAN Miniport (Network Monitor)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-Bh
Hardware ID	ms_ndiswanbh

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (PPPOE)]

Device Properties:

Driver Description	WAN Miniport (PPPOE)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-Pppoe
Hardware ID	ms_pppoeminiport

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (PPTP)]

Device Properties:

Driver Description	WAN Miniport (PPTP)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netrasa.inf
INF Section	Ndi-Mp-Pptp
Hardware ID	ms_pptpminiport

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Network adapters / WAN Miniport (SSTP)]

Device Properties:

Driver Description	WAN Miniport (SSTP)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	netsstpa.inf

INF Section	Ndi-Mp-Sstp
Hardware ID	ms_sstpminiport

Navigation

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Portable Devices / SMJ320H]

Device Properties:

Driver Description	SMJ320H
Driver Date	2/16/2012
Driver Version	2.9.317.215
Driver Provider	SAMSUNG Electronics Co., Ltd.
INF File	oem41.inf
INF Section	ssud.Install
Hardware ID	USB\VID_04E8&PID_6860&REV_0400&MS_COMP_MTP&SAMSUNG_Android

[Ports (COM & LPT) / Bluetooth SPP Driver (COM4)]

Device Properties:

Driver Description	Bluetooth SPP Driver (COM4)
Driver Date	12/22/2011
Driver Version	2.1.51.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem11.inf
INF Section	csrserial_Device.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\csrserial_1101
Location Information	CsrBtPort Bus 0

[Ports (COM & LPT) / Bluetooth SPP Driver (COM5)]

Device Properties:

Driver Description	Bluetooth SPP Driver (COM5)
Driver Date	12/22/2011
Driver Version	2.1.51.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem11.inf
INF Section	csrserial_Device.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\csrserial_1101
Location Information	CsrBtPort Bus 0

[Ports (COM & LPT) / Communications Port (COM1)]

Device Properties:

Driver Description	Communications Port (COM1)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	msports.inf
INF Section	ComPort.NT
Hardware ID	ACPI\VEN_PNP&DEV_0501

Device Resources:

IRQ	04

Port	03F8-03FF

Navigation

[Ports (COM & LPT) / Printer Port (LPT1)]

Device Properties:

Driver Description	Printer Port (LPT1)
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	msports.inf
INF Section	LptPort.NT
Hardware ID	ACPI\VEN_PNP&DEV_0400

Device Resources:

Port	0378-037F

[Print queues / Fax]

Device Properties:

Driver Description	Fax
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	printqueue.inf
INF Section	NO_DRV_LOCAL
Hardware ID	PRINTENUM\microsoftmicrosoft_s7d14

[Print queues / Microsoft Print to PDF]

Device Properties:

Driver Description	Microsoft Print to PDF
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	printqueue.inf
INF Section	NO_DRV_LOCAL
Hardware ID	PRINTENUM\{084f01fa-e634-4d77-83ee-074817c03581}

[Print queues / Microsoft XPS Document Writer]

Device Properties:

Driver Description	Microsoft XPS Document Writer
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	printqueue.inf
INF Section	NO_DRV_LOCAL
Hardware ID	PRINTENUM\{0f4130dd-19c7-7ab6-99a1-980f03b2ee4e}

[Print queues / OneNote for Windows 10]

Device Properties:

Driver Description	OneNote for Windows 10
Driver Date	6/21/2006

Navigation

Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	printqueue.inf
INF Section	NO_DRV_LOCAL
Hardware ID	PRINTENUM\{133619e4-143b-463a-b809-b1f51d05f973}

[Print queues / Root Print Queue]

Device Properties:

Driver Description	Root Print Queue
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	printqueue.inf
INF Section	NO_DRV_LOCAL
Hardware ID	PRINTENUM\LocalPrintQueue

[Print queues / Send To OneNote 2016]

Device Properties:

Driver Description	Send To OneNote 2016
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	printqueue.inf
INF Section	NO_DRV_LOCAL
Hardware ID	PRINTENUM\{3ee39114-30b4-45a4-a109-19d4a40fcc22}

[Processors / Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
Driver Date	4/21/2009
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	cpu.inf
INF Section	IntelPPM_Inst.NT
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	https://ark.intel.com/content/www/us/en/ark/search.html?q=Intel%20Core%20i3-3220
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Processors / Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
Driver Date	4/21/2009
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	cpu.inf
INF Section	IntelPPM_Inst.NT
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

Navigation

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	https://ark.intel.com/content/www/us/en/ark/search.html?q=Intel%20Core%20i3-3220
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Processors / Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
Driver Date	4/21/2009
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	cpu.inf
INF Section	IntelPPM_Inst.NT
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	https://ark.intel.com/content/www/us/en/ark/search.html?q=Intel%20Core%20i3-3220
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Processors / Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
Driver Date	4/21/2009
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	cpu.inf
INF Section	IntelPPM_Inst.NT
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	https://ark.intel.com/content/www/us/en/ark/search.html?q=Intel%20Core%20i3-3220
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[SAMSUNG Android Phone / SAMSUNG Android ADB Interface]

Device Properties:

Driver Description	SAMSUNG Android ADB Interface
Driver Date	5/6/2020
Driver Version	2.16.15.0
Driver Provider	SAMSUNG Electronics Co., Ltd.
INF File	oem28.inf
INF Section	ssud.Install.NT
Hardware ID	USB\VID_04E8&PID_6860&REV_0400&ADB

[Software devices / Microsoft Device Association Root Enumerator]

Device Properties:

Driver Description	Microsoft Device Association Root Enumerator
Driver Date	6/21/2006

Navigation

Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	c_swdevice.inf
INF Section	SoftwareDevice

[Software devices / Microsoft GS Wavetable Synth]

Device Properties:

Driver Description	Microsoft GS Wavetable Synth
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	c_swdevice.inf
INF Section	SoftwareDevice

[Software devices / Microsoft Radio Device Enumeration Bus]

Device Properties:

Driver Description	Microsoft Radio Device Enumeration Bus
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	c_swdevice.inf
INF Section	SoftwareDevice

[Software devices / Microsoft RRAS Root Enumerator]

Device Properties:

Driver Description	Microsoft RRAS Root Enumerator
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	c_swdevice.inf
INF Section	SoftwareDevice

[Sound, video and game controllers / Bluetooth Hands-free Audio Device]

Device Properties:

Driver Description	Bluetooth Hands-free Audio Device
Driver Date	2/23/2012
Driver Version	2.1.60.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem50.inf
INF Section	CsrBthAudioHF.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrBthAudioHFMini_111E
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Sound, video and game controllers / Bluetooth Hands-free Audio Device]

Device Properties:

Driver Description	Bluetooth Hands-free Audio Device

Navigation

Driver Date	2/23/2012
Driver Version	2.1.60.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem50.inf
INF Section	CsrBthAudioHF.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrBthAudioHFMini_111E
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Sound, video and game controllers / Bluetooth Stereo Audio]

Device Properties:

Driver Description	Bluetooth Stereo Audio
Driver Date	2/23/2012
Driver Version	2.1.60.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem6.inf
INF Section	AVFilter.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrAVMini_110B
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Sound, video and game controllers / Bluetooth Stereo Audio]

Device Properties:

Driver Description	Bluetooth Stereo Audio
Driver Date	2/23/2012
Driver Version	2.1.60.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem6.inf
INF Section	AVFilter.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrAVMini_110B
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Sound, video and game controllers / Bluetooth Stereo Audio]

Device Properties:

Driver Description	Bluetooth Stereo Audio
Driver Date	2/23/2012
Driver Version	2.1.60.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem6.inf
INF Section	AVFilter.NT
Hardware ID	{128CFE23-5667-45db-9C1B-23370DA73831}\CsrAVMini_110B
Location Information	CsrBtPort Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

Navigation

[Sound, video and game controllers / Krisp]

Device Properties:

Driver Description	Krisp
Driver Date	7/18/2020
Driver Version	0.8.3.0
Driver Provider	Krisp Technologies, Inc
INF File	oem9.inf
INF Section	Krisp_VAD.NT
Hardware ID	ROOT\KrispSimple

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Sound, video and game controllers / Realtek High Definition Audio]

Device Properties:

Driver Description	Realtek High Definition Audio
Driver Date	7/2/2019
Driver Version	6.0.8746.1
Driver Provider	Realtek Semiconductor Corp.
INF File	oem19.inf
INF Section	IntcAzAudModel.NTamd64
Hardware ID	HDAUDIO\FUNC_01&VEN_10EC&DEV_0269&SUBSYS_10CF9000&REV_1001
Location Information	Internal High Definition Audio Bus

Device Manufacturer:

Company Name	Realtek Semiconductor Corp.
Product Information	https://www.realtek.com/products
Driver Download	https://www.realtek.com/downloads
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Sound, video and game controllers / WO Mic Device]

Device Properties:

Driver Description	WO Mic Device
Driver Date	6/28/2019
Driver Version	1.6.0.0
Driver Provider	Wolicheng Tech Ltd.
INF File	oem34.inf
INF Section	WOVAD_MicArray.NT
Hardware ID	*WOMic

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Storage controllers / Microsoft Storage Spaces Controller]

Device Properties:

Driver Description	Microsoft Storage Spaces Controller
Driver Date	6/21/2006
Driver Version	10.0.19041.423

Driver Provider	Microsoft
INF File	spaceport.inf
INF Section	Spaceport_Install
Hardware ID	Root\Spaceport

Device Manufacturer:

Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Storage volumes / Volume]

Device Properties:

Driver Description	Volume
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	volume.inf
INF Section	volume_install.NT
Hardware ID	STORAGE\Volume

[Storage volumes / Volume]

Device Properties:

Driver Description	Volume
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	volume.inf
INF Section	volume_install.NT
Hardware ID	STORAGE\Volume

[System devices / ACPI Fixed Feature Button]

Device Properties:

Driver Description	ACPI Fixed Feature Button
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV
Hardware ID	ACPI\FixedButton

[System devices / ACPI Power Button]

Device Properties:

Driver Description	ACPI Power Button
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV
Hardware ID	ACPI\VEN_PNP&DEV_0C0C

[System devices / Composite Bus Enumerator]

Navigation

Device Properties:

Driver Description	Composite Bus Enumerator
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	compositebus.inf
INF Section	CompositeBus_Device.NT
Hardware ID	ROOT\CompositeBus

[System devices / Direct memory access controller]

Device Properties:

Driver Description	Direct memory access controller
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_X
Hardware ID	ACPI\VEN_PNP&DEV_0200

[System devices / Fujitsu FUJ02E3 Device Driver]

Device Properties:

Driver Description	Fujitsu FUJ02E3 Device Driver
Driver Date	6/30/2020
Driver Version	4.3.0.1
Driver Provider	FUJITSU CLIENT COMPUTING LIMITED
INF File	oem24.inf
INF Section	FUJ02E3_Device.NT
Hardware ID	ACPI\VEN_FUJ&DEV_02E3

[System devices / High Definition Audio Controller]

Device Properties:

Driver Description	High Definition Audio Controller
Driver Date	12/6/2019
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	hdaudbus.inf
INF Section	HDAudio_Device.NT
Hardware ID	PCI\VEN_8086&DEV_1E20&SUBSYS_176C10CF&REV_04
Location Information	PCI bus 0, device 27, function 0
PCI Device	Intel Panther Point PCH - High Definition Audio Controller [C1]

Device Resources:

IRQ	22
Memory	F7C10000-F7C13FFF

[System devices / High Precision Event Timer]

Device Properties:

Driver Description	High Precision Event Timer
Driver Date	9/15/2006
Driver Version	7.0.0.1011

Driver Provider	Intel
INF File	oem54.inf
INF Section	NO_DRV
Hardware ID	ACPI\VEN_PNP&DEV_0103

Navigation

[System devices / Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10
Driver Date	1/2/2018
Driver Version	10.1.1.45
Driver Provider	INTEL
INF File	oem3.inf
INF Section	Needs_PCI_DRV
Hardware ID	PCI\VEN_8086&DEV_1E10&SUBSYS_175810CF&REV_C4
Location Information	PCI bus 0, device 28, function 0
PCI Device	Intel Panther Point PCH - PCI Express Port 1 [C1]

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[System devices / Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12
Driver Date	1/2/2018
Driver Version	10.1.1.45
Driver Provider	INTEL
INF File	oem3.inf
INF Section	Needs_PCI_DRV
Hardware ID	PCI\VEN_8086&DEV_1E12&SUBSYS_175810CF&REV_C4
Location Information	PCI bus 0, device 28, function 1
PCI Device	Intel Panther Point PCH - PCI Express Port 2 [C1]

Device Resources:

Memory	F0000000-F00FFFFF
Port	E000-EFFF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[System devices / Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1E22]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1E22
Driver Date	1/2/2018

Navigation

Driver Version	10.1.1.45
Driver Provider	INTEL
INF File	oem3.inf
INF Section	Needs_NO_DRV
Hardware ID	PCI\VEN_8086&DEV_1E22&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 31, function 3
PCI Device	Intel Panther Point PCH - SMBus Controller [C1]

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[System devices / Intel(R) 82801 PCI Bridge - 244E]

Device Properties:

Driver Description	Intel(R) 82801 PCI Bridge - 244E
Driver Date	9/15/2006
Driver Version	7.0.0.1011
Driver Provider	Intel
INF File	oem54.inf
INF Section	PCI_DRV
Hardware ID	PCI\VEN_8086&DEV_244E&SUBSYS_175810CF&REV_A4
Location Information	PCI bus 0, device 30, function 0
PCI Device	Intel 82801xx I/O Controller Hub

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[System devices / Intel(R) B75 Express Chipset LPC Controller - 1E49]

Device Properties:

Driver Description	Intel(R) B75 Express Chipset LPC Controller - 1E49
Driver Date	1/2/2018
Driver Version	10.1.1.45
Driver Provider	INTEL
INF File	oem3.inf
INF Section	Needs_ISAPNP_DRV
Hardware ID	PCI\VEN_8086&DEV_1E49&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 31, function 0
PCI Device	Intel B75 Chipset - LPC Interface Controller [C1]

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[System devices / Intel(R) Management Engine Interface]

Navigation

Device Properties:

Driver Description	Intel(R) Management Engine Interface
Driver Date	3/28/2016
Driver Version	11.0.5.1189
Driver Provider	Intel
INF File	oem2.inf
INF Section	TEE_DDI_W10_x64
Hardware ID	PCI\VEN_8086&DEV_1E3A&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 22, function 0
PCI Device	Intel Panther Point PCH - Host Embedded Controller Interface 1 (HECI1) [C1]

Device Resources:

IRQ	65536
Memory	F7C1B000-F7C1B00F

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[System devices / Legacy device]

Device Properties:

Driver Description	Legacy device
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MEM
Hardware ID	ACPI\VEN_INT&DEV_0800

[System devices / Microsoft ACPI-Compliant System]

Device Properties:

Driver Description	Microsoft ACPI-Compliant System
Driver Date	6/21/2006
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	acpi.inf
INF Section	ACPI_Inst.NT
Hardware ID	ACPI_HAL\PNP0C08
PnP Device	ACPI Driver/BIOS

Device Resources:

IRQ	100
IRQ	101
IRQ	102
IRQ	103
IRQ	104
IRQ	105

IRQ	106
IRQ	107
IRQ	108
IRQ	109
IRQ	110
IRQ	111
IRQ	112
IRQ	113
IRQ	114
IRQ	115
IRQ	116
IRQ	117
IRQ	118
IRQ	119
IRQ	120
IRQ	121
IRQ	122
IRQ	123
IRQ	124
IRQ	125
IRQ	126
IRQ	127
IRQ	128
IRQ	129
IRQ	130
IRQ	131
IRQ	132
IRQ	133
IRQ	134
IRQ	135
IRQ	136
IRQ	137
IRQ	138
IRQ	139
IRQ	140
IRQ	141
IRQ	142
IRQ	143
IRQ	144
IRQ	145
IRQ	146
IRQ	147
IRQ	148
IRQ	149
IRQ	150
IRQ	151
IRQ	152
IRQ	153
IRQ	154
IRQ	155
IRQ	156
IRQ	157
IRQ	158
IRQ	159
IRQ	160

Navigation

IRQ	161
IRQ	162
IRQ	163
IRQ	164
IRQ	165
IRQ	166
IRQ	167
IRQ	168
IRQ	169
IRQ	170
IRQ	171
IRQ	172
IRQ	173
IRQ	174
IRQ	175
IRQ	176
IRQ	177
IRQ	178
IRQ	179
IRQ	180
IRQ	181
IRQ	182
IRQ	183
IRQ	184
IRQ	185
IRQ	186
IRQ	187
IRQ	188
IRQ	189
IRQ	190
IRQ	191
IRQ	192
IRQ	193
IRQ	194
IRQ	195
IRQ	196
IRQ	197
IRQ	198
IRQ	199
IRQ	200
IRQ	201
IRQ	202
IRQ	203
IRQ	204
IRQ	256
IRQ	257
IRQ	258
IRQ	259
IRQ	260
IRQ	261
IRQ	262
IRQ	263
IRQ	264
IRQ	265
IRQ	266

Navigation

IRQ	267
IRQ	268
IRQ	269
IRQ	270
IRQ	271
IRQ	272
IRQ	273
IRQ	274
IRQ	275
IRQ	276
IRQ	277
IRQ	278
IRQ	279
IRQ	280
IRQ	281
IRQ	282
IRQ	283
IRQ	284
IRQ	285
IRQ	286
IRQ	287
IRQ	288
IRQ	289
IRQ	290
IRQ	291
IRQ	292
IRQ	293
IRQ	294
IRQ	295
IRQ	296
IRQ	297
IRQ	298
IRQ	299
IRQ	300
IRQ	301
IRQ	302
IRQ	303
IRQ	304
IRQ	305
IRQ	306
IRQ	307
IRQ	308
IRQ	309
IRQ	310
IRQ	311
IRQ	312
IRQ	313
IRQ	314
IRQ	315
IRQ	316
IRQ	317
IRQ	318
IRQ	319
IRQ	320
IRQ	321

Navigation

IRQ	322
IRQ	323
IRQ	324
IRQ	325
IRQ	326
IRQ	327
IRQ	328
IRQ	329
IRQ	330
IRQ	331
IRQ	332
IRQ	333
IRQ	334
IRQ	335
IRQ	336
IRQ	337
IRQ	338
IRQ	339
IRQ	340
IRQ	341
IRQ	342
IRQ	343
IRQ	344
IRQ	345
IRQ	346
IRQ	347
IRQ	348
IRQ	349
IRQ	350
IRQ	351
IRQ	352
IRQ	353
IRQ	354
IRQ	355
IRQ	356
IRQ	357
IRQ	358
IRQ	359
IRQ	360
IRQ	361
IRQ	362
IRQ	363
IRQ	364
IRQ	365
IRQ	366
IRQ	367
IRQ	368
IRQ	369
IRQ	370
IRQ	371
IRQ	372
IRQ	373
IRQ	374
IRQ	375
IRQ	376

Navigation

IRQ	377
IRQ	378
IRQ	379
IRQ	380
IRQ	381
IRQ	382
IRQ	383
IRQ	384
IRQ	385
IRQ	386
IRQ	387
IRQ	388
IRQ	389
IRQ	390
IRQ	391
IRQ	392
IRQ	393
IRQ	394
IRQ	395
IRQ	396
IRQ	397
IRQ	398
IRQ	399
IRQ	400
IRQ	401
IRQ	402
IRQ	403
IRQ	404
IRQ	405
IRQ	406
IRQ	407
IRQ	408
IRQ	409
IRQ	410
IRQ	411
IRQ	412
IRQ	413
IRQ	414
IRQ	415
IRQ	416
IRQ	417
IRQ	418
IRQ	419
IRQ	420
IRQ	421
IRQ	422
IRQ	423
IRQ	424
IRQ	425
IRQ	426
IRQ	427
IRQ	428
IRQ	429
IRQ	430
IRQ	431

Navigation

IRQ	432
IRQ	433
IRQ	434
IRQ	435
IRQ	436
IRQ	437
IRQ	438
IRQ	439
IRQ	440
IRQ	441
IRQ	442
IRQ	443
IRQ	444
IRQ	445
IRQ	446
IRQ	447
IRQ	448
IRQ	449
IRQ	450
IRQ	451
IRQ	452
IRQ	453
IRQ	454
IRQ	455
IRQ	456
IRQ	457
IRQ	458
IRQ	459
IRQ	460
IRQ	461
IRQ	462
IRQ	463
IRQ	464
IRQ	465
IRQ	466
IRQ	467
IRQ	468
IRQ	469
IRQ	470
IRQ	471
IRQ	472
IRQ	473
IRQ	474
IRQ	475
IRQ	476
IRQ	477
IRQ	478
IRQ	479
IRQ	480
IRQ	481
IRQ	482
IRQ	483
IRQ	484
IRQ	485
IRQ	486

Navigation

IRQ	487
IRQ	488
IRQ	489
IRQ	490
IRQ	491
IRQ	492
IRQ	493
IRQ	494
IRQ	495
IRQ	496
IRQ	497
IRQ	498
IRQ	499
IRQ	500
IRQ	501
IRQ	502
IRQ	503
IRQ	504
IRQ	505
IRQ	506
IRQ	507
IRQ	508
IRQ	509
IRQ	510
IRQ	511
IRQ	55
IRQ	56
IRQ	57
IRQ	58
IRQ	59
IRQ	60
IRQ	61
IRQ	62
IRQ	63
IRQ	64
IRQ	65
IRQ	66
IRQ	67
IRQ	68
IRQ	69
IRQ	70
IRQ	71
IRQ	72
IRQ	73
IRQ	74
IRQ	75
IRQ	76
IRQ	77
IRQ	78
IRQ	79
IRQ	80
IRQ	81
IRQ	82
IRQ	83
IRQ	84

Navigation

IRQ	85
IRQ	86
IRQ	87
IRQ	88
IRQ	89
IRQ	90
IRQ	91
IRQ	92
IRQ	93
IRQ	94
IRQ	95
IRQ	96
IRQ	97
IRQ	98
IRQ	99

Navigation

[System devices / Microsoft Basic Display Driver]

Device Properties:

Driver Description	Microsoft Basic Display Driver
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	basicdisplay.inf
INF Section	MSBDD_Fallback
Hardware ID	ROOT\BasicDisplay

[System devices / Microsoft Basic Render Driver]

Device Properties:

Driver Description	Microsoft Basic Render Driver
Driver Date	6/21/2006
Driver Version	10.0.19041.84
Driver Provider	Microsoft
INF File	basicrender.inf
INF Section	BasicRender
Hardware ID	ROOT\BasicRender

[System devices / Microsoft Hyper-V Virtualization Infrastructure Driver]

Device Properties:

Driver Description	Microsoft Hyper-V Virtualization Infrastructure Driver
Driver Date	6/21/2006
Driver Version	10.0.19041.423
Driver Provider	Microsoft
INF File	wvid.inf
INF Section	Vid_Device_Client.NT
Hardware ID	ROOT\VID

[System devices / Microsoft System Management BIOS Driver]

Device Properties:

Driver Description	Microsoft System Management BIOS Driver
Driver Date	6/21/2006

Navigation

Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	mssmbios.inf
INF Section	MSSMBIOS_DRV
Hardware ID	ROOT\mssmbios

[System devices / Microsoft Virtual Drive Enumerator]

Device Properties:

Driver Description	Microsoft Virtual Drive Enumerator
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	vdrvroot.inf
INF Section	VDRVROOT
Hardware ID	ROOT\vdrvroot

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_PNP&DEV_0C02

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_PNP&DEV_0C02

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_INT&DEV_3F0D

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources

Navigation

Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_PNP&DEV_0C02

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_PNP&DEV_0C02

[System devices / NDIS Virtual Network Adapter Enumerator]

Device Properties:

Driver Description	NDIS Virtual Network Adapter Enumerator
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	ndisvirtualbus.inf
INF Section	NdisVirtualBus_Device.NT
Hardware ID	ROOT\NdisVirtualBus

[System devices / Numeric data processor]

Device Properties:

Driver Description	Numeric data processor
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_X
Hardware ID	ACPI\VEN_PNP&DEV_0C04

[System devices / PCI Express Root Complex]

Device Properties:

Driver Description	PCI Express Root Complex
Driver Date	6/21/2006
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	pci.inf
INF Section	PCI_ROOT
Hardware ID	ACPI\VEN_PNP&DEV_0A08

Device Resources:

Memory	000A0000-000BFFFF
Memory	000D0000-000D3FFF

Navigation

Memory	000D4000-000D7FFF
Memory	000D8000-000DBFFF
Memory	000DC000-000DFFFF
Memory	000E0000-000E3FFF
Memory	000E4000-000E7FFF
Memory	DFA00000-FEAFFFFF
Port	0000-0CF7
Port	0D00-FFFF

[System devices / Plug and Play Software Device Enumerator]

Device Properties:

Driver Description	Plug and Play Software Device Enumerator
Driver Date	12/6/2019
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	swenum.inf
INF Section	SWENUM
Hardware ID	ROOT\SWENUM

[System devices / Printer Port Logical Interface]

Device Properties:

Driver Description	Printer Port Logical Interface
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV
Hardware ID	LPTENUM\MicrosoftRawPort958A
Location Information	LPT1

[System devices / Programmable interrupt controller]

Device Properties:

Driver Description	Programmable interrupt controller
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_PIC
Hardware ID	ACPI\VEN_PNP&DEV_0000

[System devices / Remote Desktop Device Redirector Bus]

Device Properties:

Driver Description	Remote Desktop Device Redirector Bus
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	rdpbus.inf
INF Section	RDPBUS
Hardware ID	ROOT\RDPBUS

[System devices / System board]

Navigation

Device Properties:

Driver Description	System board
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_PNP&DEV_0C01

[System devices / System board]

Device Properties:

Driver Description	System board
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_MBRES
Hardware ID	ACPI\VEN_PNP&DEV_0C01

[System devices / System CMOS/real time clock]

Device Properties:

Driver Description	System CMOS/real time clock
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_X
Hardware ID	ACPI\VEN_PNP&DEV_0B00

Device Resources:

IRQ	08
Port	0070-0077

[System devices / System timer]

Device Properties:

Driver Description	System timer
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	machine.inf
INF Section	NO_DRV_X
Hardware ID	ACPI\VEN_PNP&DEV_0100

[System devices / UMBus Root Bus Enumerator]

Device Properties:

Driver Description	UMBus Root Bus Enumerator
Driver Date	6/21/2006
Driver Version	10.0.19041.1

Driver Provider	Microsoft
INF File	umbus.inf
INF Section	UmBusRoot_Device.NT
Hardware ID	root\umbus

Navigation

[System devices / Volume Manager]

Device Properties:

Driver Description	Volume Manager
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	volmgr.inf
INF Section	Volmgr
Hardware ID	ROOT\VOLMGR

[System devices / Xeon(R) processor E3 - 1200 v2/3rd Gen Core processor DRAM Controller - 0150]

Device Properties:

Driver Description	Xeon(R) processor E3 - 1200 v2/3rd Gen Core processor DRAM Controller - 0150
Driver Date	1/2/2018
Driver Version	10.1.1.45
Driver Provider	INTEL
INF File	oem35.inf
INF Section	Needs_NO_DRV
Hardware ID	PCI\VEN_8086&DEV_0150&SUBSYS_175810CF&REV_09
Location Information	PCI bus 0, device 0, function 0
PCI Device	Intel Ivy Bridge-DT - Host Bridge/DRAM Controller

[Universal Serial Bus controllers / CSR BlueCore Device]

Device Properties:

Driver Description	CSR BlueCore Device
Driver Date	2/23/2012
Driver Version	2.1.60.0
Driver Provider	Cambridge Silicon Radio Limited
INF File	oem49.inf
INF Section	csrusb.Dev.NT
Hardware ID	USB\VID_0A12&PID_0001&REV_8891
Location Information	Port_#0003.Hub_#0003

[Universal Serial Bus controllers / Generic USB Hub]

Device Properties:

Driver Description	Generic USB Hub
Driver Date	6/21/2006
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	usb.inf
INF Section	StandardHub.Dev.NT
Hardware ID	USB\VID_8087&PID_0024&REV_0000
Location Information	Port_#0001.Hub_#0001

[Universal Serial Bus controllers / Generic USB Hub]

Navigation

Device Properties:

Driver Description	Generic USB Hub
Driver Date	6/21/2006
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	usb.inf
INF Section	StandardHub.Dev.NT
Hardware ID	USB\VID_8087&PID_0024&REV_0000
Location Information	Port_#0001.Hub_#0002

[Universal Serial Bus controllers / Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
Driver Date	7/31/2013
Driver Version	9.3.0.1030
Driver Provider	Intel
INF File	oem42.inf
INF Section	Intel_EHCI.Dev.NT
Hardware ID	PCI\VEN_8086&DEV_1E26&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 29, function 0
PCI Device	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C1]

Device Resources:

IRQ	23
Memory	F7C17000-F7C173FF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Universal Serial Bus controllers / Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
Driver Date	7/31/2013
Driver Version	9.3.0.1030
Driver Provider	Intel
INF File	oem42.inf
INF Section	Intel_EHCI.Dev.NT
Hardware ID	PCI\VEN_8086&DEV_1E2D&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 26, function 0
PCI Device	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C1]

Device Resources:

IRQ	16
Memory	F7C18000-F7C183FF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets

Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

Navigation

[Universal Serial Bus controllers / Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)]

Device Properties:

Driver Description	Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
Driver Date	9/1/2020
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	usbxhci.inf
INF Section	Generic.Install.NT
Hardware ID	PCI\VEN_8086&DEV_1E31&SUBSYS_175810CF&REV_04
Location Information	PCI bus 0, device 20, function 0
PCI Device	Intel Panther Point PCH - USB 3.0 xHCI Controller [C1]

Device Resources:

IRQ	65536
Memory	F7C00000-F7C0FFFF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/goto/?p=biosupdates
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Universal Serial Bus controllers / SAMSUNG Mobile USB Composite Device]

Device Properties:

Driver Description	SAMSUNG Mobile USB Composite Device
Driver Date	5/6/2020
Driver Version	2.16.15.0
Driver Provider	SAMSUNG Electronics Co., Ltd.
INF File	oem33.inf
INF Section	ssud.Install.NT
Hardware ID	USB\VID_04E8&PID_6860&REV_0400
Location Information	Port_#0006.Hub_#0005

[Universal Serial Bus controllers / USB Composite Device]

Device Properties:

Driver Description	USB Composite Device
Driver Date	6/21/2006
Driver Version	10.0.19041.488
Driver Provider	Microsoft
INF File	usb.inf
INF Section	Composite.Dev.NT
Hardware ID	USB\VID_04D9&PID_1503&REV_0403
Location Information	Port_#0001.Hub_#0004

[Universal Serial Bus controllers / USB Root Hub (USB 3.0)]

Navigation

Device Properties:

Driver Description	USB Root Hub (USB 3.0)
Driver Date	5/9/2020
Driver Version	10.0.19041.264
Driver Provider	Microsoft
INF File	usbhub3.inf
INF Section	Generic.Install.NT
Hardware ID	USB\ROOT_HUB30&VID8086&PID1E31&REV0004

[Universal Serial Bus controllers / USB Root Hub]

Device Properties:

Driver Description	USB Root Hub
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	usbport.inf
INF Section	ROOTHUB.Dev.NT
Hardware ID	USB\ROOT_HUB20&VID8086&PID1E2D&REV0004

[Universal Serial Bus controllers / USB Root Hub]

Device Properties:

Driver Description	USB Root Hub
Driver Date	6/21/2006
Driver Version	10.0.19041.1
Driver Provider	Microsoft
INF File	usbport.inf
INF Section	ROOTHUB.Dev.NT
Hardware ID	USB\ROOT_HUB20&VID8086&PID1E26&REV0004

[Unknown / Unknown]

Device Properties:

Driver Description	Unknown

Physical Devices

PCI Devices:

Bus 0, Device 30, Function 0	Intel 82801xx I/O Controller Hub
Bus 0, Device 31, Function 0	Intel B75 Chipset - LPC Interface Controller [C1]
Bus 0, Device 0, Function 0	Intel Ivy Bridge-DT - Host Bridge/DRAM Controller
Bus 0, Device 2, Function 0	Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)
Bus 0, Device 27, Function 0	Intel Panther Point PCH - High Definition Audio Controller [C1]
Bus 0, Device 22, Function 0	Intel Panther Point PCH - Host Embedded Controller Interface 1 (HECI1) [C1]
Bus 0, Device 28, Function 0	Intel Panther Point PCH - PCI Express Port 1 [C1]
Bus 0, Device 28, Function 1	Intel Panther Point PCH - PCI Express Port 2 [C1]
Bus 0, Device 31, Function 2	Intel Panther Point PCH - SATA AHCI Controller [C1]
Bus 0, Device 31, Function 3	Intel Panther Point PCH - SMBus Controller [C1]
Bus 0, Device 31, Function 6	Intel Panther Point PCH - Thermal Management Controller [C1]
Bus 0, Device 29, Function 0	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C1]
Bus 0, Device 26, Function 0	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C1]

Bus 0, Device 20, Function 0	Intel Panther Point PCH - USB
Bus 2, Device 0, Function 0	Realtek RTL8168/8111 PCI-E G

PnP Devices:

PNP0501	16550A-compatible UART Serial Port
PNP0C08	ACPI Driver/BIOS
FIXEDBUTTON	ACPI Fixed Feature Button
PNP0A08	ACPI Three-wire Device Bus
PNP0200	DMA Controller
FUJ02E3	Fujitsu FUJ02E3 Device
PNP0103	High Precision Event Timer
INT0800	Intel Flash EEPROM
INT3F0D	Intel Watchdog Timer
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-_____INTEL(R)_CORE(TM)_I3-3220_CPU_@_3.30GHZ	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-_____INTEL(R)_CORE(TM)_I3-3220_CPU_@_3.30GHZ	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-_____INTEL(R)_CORE(TM)_I3-3220_CPU_@_3.30GHZ	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-_____INTEL(R)_CORE(TM)_I3-3220_CPU_@_3.30GHZ	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
PNP0C04	Numeric Data Processor
PNP0400	Parallel Port
PNP0C0C	Power Button
PNP0000	Programmable Interrupt Controller
PNP0B00	Real-Time Clock
PNP0C01	System Board Extension
PNP0C01	System Board Extension
PNP0100	System Timer
PNP0C02	Thermal Monitoring ACPI Device
PNP0C02	Thermal Monitoring ACPI Device
PNP0C02	Thermal Monitoring ACPI Device
PNP0C02	Thermal Monitoring ACPI Device

LPT PnP Devices:

MICROSOFTRAWPORT	Printer Port Logical Interface

USB Devices:

0A12 0001	CSR BlueCore Device
8087 0024	Generic USB Hub
8087 0024	Generic USB Hub
04E8 6860	SAMSUNG Android ADB Interface
04E8 6860	SAMSUNG Mobile USB Composite Device
04E8 6860	SAMSUNG Mobile USB Modem
04E8 6860	SMJ320H
04D9 1503	USB Composite Device
04D9 1503	USB Input Device
04D9 1503	USB Input Device
093A 2510	USB Input Device

Ports:

COM1	Communications Port (COM1)
COM4	Bluetooth SPP Driver (COM4)
COM5	Bluetooth SPP Driver (COM5)
LPT1	Printer Port (LPT1)

PCI Devices

Navigation

[Intel 82801xx I/O Controller Hub]

Device Properties:

Device Description	Intel 82801xx I/O Controller Hub
Bus Type	PCI
Bus / Device / Function	0 / 30 / 0
Device ID	8086-244E
Subsystem ID	0000-0000
Device Class	0604 (PCI/PCI Bridge)
Revision	A4
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel B75 Chipset - LPC Interface Controller [C1]]

Device Properties:

Device Description	Intel B75 Chipset - LPC Interface Controller [C1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 0
Device ID	8086-1E49
Subsystem ID	10CF-1758
Device Class	0601 (PCI/ISA Bridge)
Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Ivy Bridge-DT - Host Bridge/DRAM Controller]

Device Properties:

Device Description	Intel Ivy Bridge-DT - Host Bridge/DRAM Controller
Bus Type	PCI
Bus / Device / Function	0 / 0 / 0
Device ID	8086-0150
Subsystem ID	10CF-1758
Device Class	0600 (Host/PCI Bridge)
Revision	09
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)]

Device Properties:

Device Description	Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)
Bus Type	PCI

Navigation

Bus / Device / Function	0 / 2 / 0
Device ID	8086-0152
Subsystem ID	10CF-176D
Device Class	0300 (VGA Display Controller)
Revision	09
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	https://www.intel.com/products/chipsets
Driver Download	https://www.intel.com/support/graphics
Driver Update	http://www.aida64.com/goto/?p=drvupdates

[Intel Panther Point PCH - High Definition Audio Controller [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - High Definition Audio Controller [C1]
Bus Type	PCI Express 1.0
Bus / Device / Function	0 / 27 / 0
Device ID	8086-1E20
Subsystem ID	10CF-176C
Device Class	0403 (High Definition Audio)
Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - Host Embedded Controller Interface 1 (HECI1) [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - Host Embedded Controller Interface 1 (HECI1) [C1]
Bus Type	PCI
Bus / Device / Function	0 / 22 / 0
Device ID	8086-1E3A
Subsystem ID	10CF-1758
Device Class	0780 (Communications Controller)
Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - PCI Express Port 1 [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - PCI Express Port 1 [C1]
Bus Type	PCI

Bus / Device / Function	0 / 28 / 0
Device ID	8086-1E10
Subsystem ID	0000-0000
Device Class	0604 (PCI/PCI Bridge)
Revision	C4
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - PCI Express Port 2 [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - PCI Express Port 2 [C1]
Bus Type	PCI
Bus / Device / Function	0 / 28 / 1
Device ID	8086-1E12
Subsystem ID	0000-0000
Device Class	0604 (PCI/PCI Bridge)
Revision	C4
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - SATA AHCI Controller [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - SATA AHCI Controller [C1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 2
Device ID	8086-1E02
Subsystem ID	10CF-1758
Device Class	0106 (SATA Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - SMBus Controller [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - SMBus Controller [C1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 3
Device ID	8086-1E22
Subsystem ID	10CF-1758
Device Class	0C05 (SMBus Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Navigation

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Disabled

[Intel Panther Point PCH - Thermal Management Controller [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - Thermal Management Controller [C1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 6
Device ID	8086-1E24
Subsystem ID	10CF-1758
Device Class	1180 (Data Acquisition / Signal Processing Controller)
Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Disabled

[Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C1]
Bus Type	PCI
Bus / Device / Function	0 / 29 / 0
Device ID	8086-1E26
Subsystem ID	10CF-1758
Device Class	0C03 (USB2 EHCI Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C1]]

Device Properties:

Device Description	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C1]
Bus Type	PCI
Bus / Device / Function	0 / 26 / 0
Device ID	8086-1E2D
Subsystem ID	10CF-1758
Device Class	0C03 (USB2 EHCI Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - USB 3.0 xHCI Controller [C1]]

Navigation

Device Properties:

Device Description	Intel Panther Point PCH - USB 3.0 xHCI Controller [C1]
Bus Type	PCI
Bus / Device / Function	0 / 20 / 0
Device ID	8086-1E31
Subsystem ID	10CF-1758
Device Class	0C03 (USB3 xHCI Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter]

Device Properties:

Device Description	Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter
Bus Type	PCI Express 2.0 x1
Bus / Device / Function	2 / 0 / 0
Device ID	10EC-8168
Subsystem ID	10CF-175A
Device Class	0200 (Ethernet Controller)
Revision	07
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

Network Adapter Manufacturer:

Company Name	Realtek Semiconductor Corp.
Product Information	https://www.realtek.com/products
Driver Download	https://www.realtek.com/downloads
Driver Update	http://www.aida64.com/goto/?p=drvupdates

USB Devices

[CSR BlueCore Device]

Device Properties:

Device Description	CSR BlueCore Device
Device ID	0A12-0001
Device Class	E0 / 01 (Bluetooth)
Device Protocol	01
Revision	8891h
Supported USB Version	2.00
Current Speed	Full (USB 1.1)

[Generic USB Hub]

Navigation

Device Properties:

Device Description	Generic USB Hub
Device ID	8087-0024
Device Class	09 / 00 (Hi-Speed Hub with single TT)
Device Protocol	01
Revision	0000h
Supported USB Version	2.00
Current Speed	High (USB 2.0)

[USB Composite Device (USB Keyboard)]

Device Properties:

Device Description	USB Composite Device
Device ID	04D9-1503
Device Class	03 / 01 (Human Interface Device)
Device Protocol	01
Revision	0403h
Product	USB Keyboard
Supported USB Version	1.10
Current Speed	Low (USB 1.1)

[USB Input Device (USB Optical Mouse)]

Device Properties:

Device Description	USB Input Device
Device ID	093A-2510
Device Class	03 / 01 (Human Interface Device)
Device Protocol	02
Revision	0100h
Manufacturer	PixArt
Product	USB Optical Mouse
Supported USB Version	1.10
Current Speed	Low (USB 1.1)

[Generic USB Hub]

Device Properties:

Device Description	Generic USB Hub
Device ID	8087-0024
Device Class	09 / 00 (Hi-Speed Hub with single TT)
Device Protocol	01
Revision	0000h
Supported USB Version	2.00
Current Speed	High (USB 2.0)

[SAMSUNG Mobile USB Composite Device (SAMSUNG_Android)]

Device Properties:

Device Description	SAMSUNG Mobile USB Composite Device
Device ID	04E8-6860
Device Class	06 / 01 (Imaging)
Device Protocol	01
Revision	0400h
Manufacturer	SAMSUNG

Product	SAMSUNG_Android
Serial Number	4200a800905f4300
Supported USB Version	2.00
Current Speed	High (USB 2.0)

Navigation

Device Resources

Resource	Share	Device Description
IRQ 04	Exclusive	Communications Port (COM1)
IRQ 08	Exclusive	System CMOS/real time clock
IRQ 100	Exclusive	Microsoft ACPI-Compliant System
IRQ 101	Exclusive	Microsoft ACPI-Compliant System
IRQ 102	Exclusive	Microsoft ACPI-Compliant System
IRQ 103	Exclusive	Microsoft ACPI-Compliant System
IRQ 104	Exclusive	Microsoft ACPI-Compliant System
IRQ 105	Exclusive	Microsoft ACPI-Compliant System
IRQ 106	Exclusive	Microsoft ACPI-Compliant System
IRQ 107	Exclusive	Microsoft ACPI-Compliant System
IRQ 108	Exclusive	Microsoft ACPI-Compliant System
IRQ 109	Exclusive	Microsoft ACPI-Compliant System
IRQ 110	Exclusive	Microsoft ACPI-Compliant System
IRQ 111	Exclusive	Microsoft ACPI-Compliant System
IRQ 112	Exclusive	Microsoft ACPI-Compliant System
IRQ 113	Exclusive	Microsoft ACPI-Compliant System
IRQ 114	Exclusive	Microsoft ACPI-Compliant System
IRQ 115	Exclusive	Microsoft ACPI-Compliant System
IRQ 116	Exclusive	Microsoft ACPI-Compliant System
IRQ 117	Exclusive	Microsoft ACPI-Compliant System
IRQ 118	Exclusive	Microsoft ACPI-Compliant System
IRQ 119	Exclusive	Microsoft ACPI-Compliant System
IRQ 120	Exclusive	Microsoft ACPI-Compliant System
IRQ 121	Exclusive	Microsoft ACPI-Compliant System
IRQ 122	Exclusive	Microsoft ACPI-Compliant System
IRQ 123	Exclusive	Microsoft ACPI-Compliant System
IRQ 124	Exclusive	Microsoft ACPI-Compliant System
IRQ 125	Exclusive	Microsoft ACPI-Compliant System
IRQ 126	Exclusive	Microsoft ACPI-Compliant System
IRQ 127	Exclusive	Microsoft ACPI-Compliant System
IRQ 128	Exclusive	Microsoft ACPI-Compliant System
IRQ 129	Exclusive	Microsoft ACPI-Compliant System
IRQ 130	Exclusive	Microsoft ACPI-Compliant System
IRQ 131	Exclusive	Microsoft ACPI-Compliant System
IRQ 132	Exclusive	Microsoft ACPI-Compliant System
IRQ 133	Exclusive	Microsoft ACPI-Compliant System
IRQ 134	Exclusive	Microsoft ACPI-Compliant System
IRQ 135	Exclusive	Microsoft ACPI-Compliant System
IRQ 136	Exclusive	Microsoft ACPI-Compliant System
IRQ 137	Exclusive	Microsoft ACPI-Compliant System
IRQ 138	Exclusive	Microsoft ACPI-Compliant System
IRQ 139	Exclusive	Microsoft ACPI-Compliant System
IRQ 140	Exclusive	Microsoft ACPI-Compliant System
IRQ 141	Exclusive	Microsoft ACPI-Compliant System
IRQ 142	Exclusive	Microsoft ACPI-Compliant System

Navigation

IRQ 143	Exclusive	Microsoft ACPI-Compliant System
IRQ 144	Exclusive	Microsoft ACPI-Compliant System
IRQ 145	Exclusive	Microsoft ACPI-Compliant System
IRQ 146	Exclusive	Microsoft ACPI-Compliant System
IRQ 147	Exclusive	Microsoft ACPI-Compliant System
IRQ 148	Exclusive	Microsoft ACPI-Compliant System
IRQ 149	Exclusive	Microsoft ACPI-Compliant System
IRQ 150	Exclusive	Microsoft ACPI-Compliant System
IRQ 151	Exclusive	Microsoft ACPI-Compliant System
IRQ 152	Exclusive	Microsoft ACPI-Compliant System
IRQ 153	Exclusive	Microsoft ACPI-Compliant System
IRQ 154	Exclusive	Microsoft ACPI-Compliant System
IRQ 155	Exclusive	Microsoft ACPI-Compliant System
IRQ 156	Exclusive	Microsoft ACPI-Compliant System
IRQ 157	Exclusive	Microsoft ACPI-Compliant System
IRQ 158	Exclusive	Microsoft ACPI-Compliant System
IRQ 159	Exclusive	Microsoft ACPI-Compliant System
IRQ 16	Shared	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
IRQ 160	Exclusive	Microsoft ACPI-Compliant System
IRQ 161	Exclusive	Microsoft ACPI-Compliant System
IRQ 162	Exclusive	Microsoft ACPI-Compliant System
IRQ 163	Exclusive	Microsoft ACPI-Compliant System
IRQ 164	Exclusive	Microsoft ACPI-Compliant System
IRQ 165	Exclusive	Microsoft ACPI-Compliant System
IRQ 166	Exclusive	Microsoft ACPI-Compliant System
IRQ 167	Exclusive	Microsoft ACPI-Compliant System
IRQ 168	Exclusive	Microsoft ACPI-Compliant System
IRQ 169	Exclusive	Microsoft ACPI-Compliant System
IRQ 17	Shared	Realtek PCIe GbE Family Controller
IRQ 170	Exclusive	Microsoft ACPI-Compliant System
IRQ 171	Exclusive	Microsoft ACPI-Compliant System
IRQ 172	Exclusive	Microsoft ACPI-Compliant System
IRQ 173	Exclusive	Microsoft ACPI-Compliant System
IRQ 174	Exclusive	Microsoft ACPI-Compliant System
IRQ 175	Exclusive	Microsoft ACPI-Compliant System
IRQ 176	Exclusive	Microsoft ACPI-Compliant System
IRQ 177	Exclusive	Microsoft ACPI-Compliant System
IRQ 178	Exclusive	Microsoft ACPI-Compliant System
IRQ 179	Exclusive	Microsoft ACPI-Compliant System
IRQ 180	Exclusive	Microsoft ACPI-Compliant System
IRQ 181	Exclusive	Microsoft ACPI-Compliant System
IRQ 182	Exclusive	Microsoft ACPI-Compliant System
IRQ 183	Exclusive	Microsoft ACPI-Compliant System
IRQ 184	Exclusive	Microsoft ACPI-Compliant System
IRQ 185	Exclusive	Microsoft ACPI-Compliant System
IRQ 186	Exclusive	Microsoft ACPI-Compliant System
IRQ 187	Exclusive	Microsoft ACPI-Compliant System
IRQ 188	Exclusive	Microsoft ACPI-Compliant System
IRQ 189	Exclusive	Microsoft ACPI-Compliant System
IRQ 190	Exclusive	Microsoft ACPI-Compliant System
IRQ 191	Exclusive	Microsoft ACPI-Compliant System
IRQ 192	Exclusive	Microsoft ACPI-Compliant System
IRQ 193	Exclusive	Microsoft ACPI-Compliant System
IRQ 194	Exclusive	Microsoft ACPI-Compliant System
IRQ 195	Exclusive	Microsoft ACPI-Compliant System

Navigation

IRQ 196	Exclusive	Microsoft ACPI-Compliant System
IRQ 197	Exclusive	Microsoft ACPI-Compliant System
IRQ 198	Exclusive	Microsoft ACPI-Compliant System
IRQ 199	Exclusive	Microsoft ACPI-Compliant System
IRQ 200	Exclusive	Microsoft ACPI-Compliant System
IRQ 201	Exclusive	Microsoft ACPI-Compliant System
IRQ 202	Exclusive	Microsoft ACPI-Compliant System
IRQ 203	Exclusive	Microsoft ACPI-Compliant System
IRQ 204	Exclusive	Microsoft ACPI-Compliant System
IRQ 22	Shared	High Definition Audio Controller
IRQ 23	Shared	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
IRQ 256	Exclusive	Microsoft ACPI-Compliant System
IRQ 257	Exclusive	Microsoft ACPI-Compliant System
IRQ 258	Exclusive	Microsoft ACPI-Compliant System
IRQ 259	Exclusive	Microsoft ACPI-Compliant System
IRQ 260	Exclusive	Microsoft ACPI-Compliant System
IRQ 261	Exclusive	Microsoft ACPI-Compliant System
IRQ 262	Exclusive	Microsoft ACPI-Compliant System
IRQ 263	Exclusive	Microsoft ACPI-Compliant System
IRQ 264	Exclusive	Microsoft ACPI-Compliant System
IRQ 265	Exclusive	Microsoft ACPI-Compliant System
IRQ 266	Exclusive	Microsoft ACPI-Compliant System
IRQ 267	Exclusive	Microsoft ACPI-Compliant System
IRQ 268	Exclusive	Microsoft ACPI-Compliant System
IRQ 269	Exclusive	Microsoft ACPI-Compliant System
IRQ 270	Exclusive	Microsoft ACPI-Compliant System
IRQ 271	Exclusive	Microsoft ACPI-Compliant System
IRQ 272	Exclusive	Microsoft ACPI-Compliant System
IRQ 273	Exclusive	Microsoft ACPI-Compliant System
IRQ 274	Exclusive	Microsoft ACPI-Compliant System
IRQ 275	Exclusive	Microsoft ACPI-Compliant System
IRQ 276	Exclusive	Microsoft ACPI-Compliant System
IRQ 277	Exclusive	Microsoft ACPI-Compliant System
IRQ 278	Exclusive	Microsoft ACPI-Compliant System
IRQ 279	Exclusive	Microsoft ACPI-Compliant System
IRQ 280	Exclusive	Microsoft ACPI-Compliant System
IRQ 281	Exclusive	Microsoft ACPI-Compliant System
IRQ 282	Exclusive	Microsoft ACPI-Compliant System
IRQ 283	Exclusive	Microsoft ACPI-Compliant System
IRQ 284	Exclusive	Microsoft ACPI-Compliant System
IRQ 285	Exclusive	Microsoft ACPI-Compliant System
IRQ 286	Exclusive	Microsoft ACPI-Compliant System
IRQ 287	Exclusive	Microsoft ACPI-Compliant System
IRQ 288	Exclusive	Microsoft ACPI-Compliant System
IRQ 289	Exclusive	Microsoft ACPI-Compliant System
IRQ 290	Exclusive	Microsoft ACPI-Compliant System
IRQ 291	Exclusive	Microsoft ACPI-Compliant System
IRQ 292	Exclusive	Microsoft ACPI-Compliant System
IRQ 293	Exclusive	Microsoft ACPI-Compliant System
IRQ 294	Exclusive	Microsoft ACPI-Compliant System
IRQ 295	Exclusive	Microsoft ACPI-Compliant System
IRQ 296	Exclusive	Microsoft ACPI-Compliant System
IRQ 297	Exclusive	Microsoft ACPI-Compliant System
IRQ 298	Exclusive	Microsoft ACPI-Compliant System
IRQ 299	Exclusive	Microsoft ACPI-Compliant System

IRQ 300	Exclusive	Microsoft ACPI-Compliant System
IRQ 301	Exclusive	Microsoft ACPI-Compliant System
IRQ 302	Exclusive	Microsoft ACPI-Compliant System
IRQ 303	Exclusive	Microsoft ACPI-Compliant System
IRQ 304	Exclusive	Microsoft ACPI-Compliant System
IRQ 305	Exclusive	Microsoft ACPI-Compliant System
IRQ 306	Exclusive	Microsoft ACPI-Compliant System
IRQ 307	Exclusive	Microsoft ACPI-Compliant System
IRQ 308	Exclusive	Microsoft ACPI-Compliant System
IRQ 309	Exclusive	Microsoft ACPI-Compliant System
IRQ 310	Exclusive	Microsoft ACPI-Compliant System
IRQ 311	Exclusive	Microsoft ACPI-Compliant System
IRQ 312	Exclusive	Microsoft ACPI-Compliant System
IRQ 313	Exclusive	Microsoft ACPI-Compliant System
IRQ 314	Exclusive	Microsoft ACPI-Compliant System
IRQ 315	Exclusive	Microsoft ACPI-Compliant System
IRQ 316	Exclusive	Microsoft ACPI-Compliant System
IRQ 317	Exclusive	Microsoft ACPI-Compliant System
IRQ 318	Exclusive	Microsoft ACPI-Compliant System
IRQ 319	Exclusive	Microsoft ACPI-Compliant System
IRQ 320	Exclusive	Microsoft ACPI-Compliant System
IRQ 321	Exclusive	Microsoft ACPI-Compliant System
IRQ 322	Exclusive	Microsoft ACPI-Compliant System
IRQ 323	Exclusive	Microsoft ACPI-Compliant System
IRQ 324	Exclusive	Microsoft ACPI-Compliant System
IRQ 325	Exclusive	Microsoft ACPI-Compliant System
IRQ 326	Exclusive	Microsoft ACPI-Compliant System
IRQ 327	Exclusive	Microsoft ACPI-Compliant System
IRQ 328	Exclusive	Microsoft ACPI-Compliant System
IRQ 329	Exclusive	Microsoft ACPI-Compliant System
IRQ 330	Exclusive	Microsoft ACPI-Compliant System
IRQ 331	Exclusive	Microsoft ACPI-Compliant System
IRQ 332	Exclusive	Microsoft ACPI-Compliant System
IRQ 333	Exclusive	Microsoft ACPI-Compliant System
IRQ 334	Exclusive	Microsoft ACPI-Compliant System
IRQ 335	Exclusive	Microsoft ACPI-Compliant System
IRQ 336	Exclusive	Microsoft ACPI-Compliant System
IRQ 337	Exclusive	Microsoft ACPI-Compliant System
IRQ 338	Exclusive	Microsoft ACPI-Compliant System
IRQ 339	Exclusive	Microsoft ACPI-Compliant System
IRQ 340	Exclusive	Microsoft ACPI-Compliant System
IRQ 341	Exclusive	Microsoft ACPI-Compliant System
IRQ 342	Exclusive	Microsoft ACPI-Compliant System
IRQ 343	Exclusive	Microsoft ACPI-Compliant System
IRQ 344	Exclusive	Microsoft ACPI-Compliant System
IRQ 345	Exclusive	Microsoft ACPI-Compliant System
IRQ 346	Exclusive	Microsoft ACPI-Compliant System
IRQ 347	Exclusive	Microsoft ACPI-Compliant System
IRQ 348	Exclusive	Microsoft ACPI-Compliant System
IRQ 349	Exclusive	Microsoft ACPI-Compliant System
IRQ 350	Exclusive	Microsoft ACPI-Compliant System
IRQ 351	Exclusive	Microsoft ACPI-Compliant System
IRQ 352	Exclusive	Microsoft ACPI-Compliant System
IRQ 353	Exclusive	Microsoft ACPI-Compliant System
IRQ 354	Exclusive	Microsoft ACPI-Compliant System

Navigation

Navigation

IRQ 355	Exclusive	Microsoft ACPI-Compliant System
IRQ 356	Exclusive	Microsoft ACPI-Compliant System
IRQ 357	Exclusive	Microsoft ACPI-Compliant System
IRQ 358	Exclusive	Microsoft ACPI-Compliant System
IRQ 359	Exclusive	Microsoft ACPI-Compliant System
IRQ 360	Exclusive	Microsoft ACPI-Compliant System
IRQ 361	Exclusive	Microsoft ACPI-Compliant System
IRQ 362	Exclusive	Microsoft ACPI-Compliant System
IRQ 363	Exclusive	Microsoft ACPI-Compliant System
IRQ 364	Exclusive	Microsoft ACPI-Compliant System
IRQ 365	Exclusive	Microsoft ACPI-Compliant System
IRQ 366	Exclusive	Microsoft ACPI-Compliant System
IRQ 367	Exclusive	Microsoft ACPI-Compliant System
IRQ 368	Exclusive	Microsoft ACPI-Compliant System
IRQ 369	Exclusive	Microsoft ACPI-Compliant System
IRQ 370	Exclusive	Microsoft ACPI-Compliant System
IRQ 371	Exclusive	Microsoft ACPI-Compliant System
IRQ 372	Exclusive	Microsoft ACPI-Compliant System
IRQ 373	Exclusive	Microsoft ACPI-Compliant System
IRQ 374	Exclusive	Microsoft ACPI-Compliant System
IRQ 375	Exclusive	Microsoft ACPI-Compliant System
IRQ 376	Exclusive	Microsoft ACPI-Compliant System
IRQ 377	Exclusive	Microsoft ACPI-Compliant System
IRQ 378	Exclusive	Microsoft ACPI-Compliant System
IRQ 379	Exclusive	Microsoft ACPI-Compliant System
IRQ 380	Exclusive	Microsoft ACPI-Compliant System
IRQ 381	Exclusive	Microsoft ACPI-Compliant System
IRQ 382	Exclusive	Microsoft ACPI-Compliant System
IRQ 383	Exclusive	Microsoft ACPI-Compliant System
IRQ 384	Exclusive	Microsoft ACPI-Compliant System
IRQ 385	Exclusive	Microsoft ACPI-Compliant System
IRQ 386	Exclusive	Microsoft ACPI-Compliant System
IRQ 387	Exclusive	Microsoft ACPI-Compliant System
IRQ 388	Exclusive	Microsoft ACPI-Compliant System
IRQ 389	Exclusive	Microsoft ACPI-Compliant System
IRQ 390	Exclusive	Microsoft ACPI-Compliant System
IRQ 391	Exclusive	Microsoft ACPI-Compliant System
IRQ 392	Exclusive	Microsoft ACPI-Compliant System
IRQ 393	Exclusive	Microsoft ACPI-Compliant System
IRQ 394	Exclusive	Microsoft ACPI-Compliant System
IRQ 395	Exclusive	Microsoft ACPI-Compliant System
IRQ 396	Exclusive	Microsoft ACPI-Compliant System
IRQ 397	Exclusive	Microsoft ACPI-Compliant System
IRQ 398	Exclusive	Microsoft ACPI-Compliant System
IRQ 399	Exclusive	Microsoft ACPI-Compliant System
IRQ 400	Exclusive	Microsoft ACPI-Compliant System
IRQ 401	Exclusive	Microsoft ACPI-Compliant System
IRQ 402	Exclusive	Microsoft ACPI-Compliant System
IRQ 403	Exclusive	Microsoft ACPI-Compliant System
IRQ 404	Exclusive	Microsoft ACPI-Compliant System
IRQ 405	Exclusive	Microsoft ACPI-Compliant System
IRQ 406	Exclusive	Microsoft ACPI-Compliant System
IRQ 407	Exclusive	Microsoft ACPI-Compliant System
IRQ 408	Exclusive	Microsoft ACPI-Compliant System
IRQ 409	Exclusive	Microsoft ACPI-Compliant System

IRQ 410	Exclusive	Microsoft ACPI-Compliant System
IRQ 411	Exclusive	Microsoft ACPI-Compliant System
IRQ 412	Exclusive	Microsoft ACPI-Compliant System
IRQ 413	Exclusive	Microsoft ACPI-Compliant System
IRQ 414	Exclusive	Microsoft ACPI-Compliant System
IRQ 415	Exclusive	Microsoft ACPI-Compliant System
IRQ 416	Exclusive	Microsoft ACPI-Compliant System
IRQ 417	Exclusive	Microsoft ACPI-Compliant System
IRQ 418	Exclusive	Microsoft ACPI-Compliant System
IRQ 419	Exclusive	Microsoft ACPI-Compliant System
IRQ 420	Exclusive	Microsoft ACPI-Compliant System
IRQ 421	Exclusive	Microsoft ACPI-Compliant System
IRQ 422	Exclusive	Microsoft ACPI-Compliant System
IRQ 423	Exclusive	Microsoft ACPI-Compliant System
IRQ 424	Exclusive	Microsoft ACPI-Compliant System
IRQ 425	Exclusive	Microsoft ACPI-Compliant System
IRQ 426	Exclusive	Microsoft ACPI-Compliant System
IRQ 427	Exclusive	Microsoft ACPI-Compliant System
IRQ 428	Exclusive	Microsoft ACPI-Compliant System
IRQ 429	Exclusive	Microsoft ACPI-Compliant System
IRQ 430	Exclusive	Microsoft ACPI-Compliant System
IRQ 431	Exclusive	Microsoft ACPI-Compliant System
IRQ 432	Exclusive	Microsoft ACPI-Compliant System
IRQ 433	Exclusive	Microsoft ACPI-Compliant System
IRQ 434	Exclusive	Microsoft ACPI-Compliant System
IRQ 435	Exclusive	Microsoft ACPI-Compliant System
IRQ 436	Exclusive	Microsoft ACPI-Compliant System
IRQ 437	Exclusive	Microsoft ACPI-Compliant System
IRQ 438	Exclusive	Microsoft ACPI-Compliant System
IRQ 439	Exclusive	Microsoft ACPI-Compliant System
IRQ 440	Exclusive	Microsoft ACPI-Compliant System
IRQ 441	Exclusive	Microsoft ACPI-Compliant System
IRQ 442	Exclusive	Microsoft ACPI-Compliant System
IRQ 443	Exclusive	Microsoft ACPI-Compliant System
IRQ 444	Exclusive	Microsoft ACPI-Compliant System
IRQ 445	Exclusive	Microsoft ACPI-Compliant System
IRQ 446	Exclusive	Microsoft ACPI-Compliant System
IRQ 447	Exclusive	Microsoft ACPI-Compliant System
IRQ 448	Exclusive	Microsoft ACPI-Compliant System
IRQ 449	Exclusive	Microsoft ACPI-Compliant System
IRQ 450	Exclusive	Microsoft ACPI-Compliant System
IRQ 451	Exclusive	Microsoft ACPI-Compliant System
IRQ 452	Exclusive	Microsoft ACPI-Compliant System
IRQ 453	Exclusive	Microsoft ACPI-Compliant System
IRQ 454	Exclusive	Microsoft ACPI-Compliant System
IRQ 455	Exclusive	Microsoft ACPI-Compliant System
IRQ 456	Exclusive	Microsoft ACPI-Compliant System
IRQ 457	Exclusive	Microsoft ACPI-Compliant System
IRQ 458	Exclusive	Microsoft ACPI-Compliant System
IRQ 459	Exclusive	Microsoft ACPI-Compliant System
IRQ 460	Exclusive	Microsoft ACPI-Compliant System
IRQ 461	Exclusive	Microsoft ACPI-Compliant System
IRQ 462	Exclusive	Microsoft ACPI-Compliant System
IRQ 463	Exclusive	Microsoft ACPI-Compliant System
IRQ 464	Exclusive	Microsoft ACPI-Compliant System

Navigation

Navigation

IRQ 465	Exclusive	Microsoft ACPI-Compliant System
IRQ 466	Exclusive	Microsoft ACPI-Compliant System
IRQ 467	Exclusive	Microsoft ACPI-Compliant System
IRQ 468	Exclusive	Microsoft ACPI-Compliant System
IRQ 469	Exclusive	Microsoft ACPI-Compliant System
IRQ 470	Exclusive	Microsoft ACPI-Compliant System
IRQ 471	Exclusive	Microsoft ACPI-Compliant System
IRQ 472	Exclusive	Microsoft ACPI-Compliant System
IRQ 473	Exclusive	Microsoft ACPI-Compliant System
IRQ 474	Exclusive	Microsoft ACPI-Compliant System
IRQ 475	Exclusive	Microsoft ACPI-Compliant System
IRQ 476	Exclusive	Microsoft ACPI-Compliant System
IRQ 477	Exclusive	Microsoft ACPI-Compliant System
IRQ 478	Exclusive	Microsoft ACPI-Compliant System
IRQ 479	Exclusive	Microsoft ACPI-Compliant System
IRQ 480	Exclusive	Microsoft ACPI-Compliant System
IRQ 481	Exclusive	Microsoft ACPI-Compliant System
IRQ 482	Exclusive	Microsoft ACPI-Compliant System
IRQ 483	Exclusive	Microsoft ACPI-Compliant System
IRQ 484	Exclusive	Microsoft ACPI-Compliant System
IRQ 485	Exclusive	Microsoft ACPI-Compliant System
IRQ 486	Exclusive	Microsoft ACPI-Compliant System
IRQ 487	Exclusive	Microsoft ACPI-Compliant System
IRQ 488	Exclusive	Microsoft ACPI-Compliant System
IRQ 489	Exclusive	Microsoft ACPI-Compliant System
IRQ 490	Exclusive	Microsoft ACPI-Compliant System
IRQ 491	Exclusive	Microsoft ACPI-Compliant System
IRQ 492	Exclusive	Microsoft ACPI-Compliant System
IRQ 493	Exclusive	Microsoft ACPI-Compliant System
IRQ 494	Exclusive	Microsoft ACPI-Compliant System
IRQ 495	Exclusive	Microsoft ACPI-Compliant System
IRQ 496	Exclusive	Microsoft ACPI-Compliant System
IRQ 497	Exclusive	Microsoft ACPI-Compliant System
IRQ 498	Exclusive	Microsoft ACPI-Compliant System
IRQ 499	Exclusive	Microsoft ACPI-Compliant System
IRQ 500	Exclusive	Microsoft ACPI-Compliant System
IRQ 501	Exclusive	Microsoft ACPI-Compliant System
IRQ 502	Exclusive	Microsoft ACPI-Compliant System
IRQ 503	Exclusive	Microsoft ACPI-Compliant System
IRQ 504	Exclusive	Microsoft ACPI-Compliant System
IRQ 505	Exclusive	Microsoft ACPI-Compliant System
IRQ 506	Exclusive	Microsoft ACPI-Compliant System
IRQ 507	Exclusive	Microsoft ACPI-Compliant System
IRQ 508	Exclusive	Microsoft ACPI-Compliant System
IRQ 509	Exclusive	Microsoft ACPI-Compliant System
IRQ 510	Exclusive	Microsoft ACPI-Compliant System
IRQ 511	Exclusive	Microsoft ACPI-Compliant System
IRQ 55	Exclusive	Microsoft ACPI-Compliant System
IRQ 56	Exclusive	Microsoft ACPI-Compliant System
IRQ 57	Exclusive	Microsoft ACPI-Compliant System
IRQ 58	Exclusive	Microsoft ACPI-Compliant System
IRQ 59	Exclusive	Microsoft ACPI-Compliant System
IRQ 60	Exclusive	Microsoft ACPI-Compliant System
IRQ 61	Exclusive	Microsoft ACPI-Compliant System
IRQ 62	Exclusive	Microsoft ACPI-Compliant System

Navigation

IRQ 63	Exclusive	Microsoft ACPI-Compliant System
IRQ 64	Exclusive	Microsoft ACPI-Compliant System
IRQ 65	Exclusive	Microsoft ACPI-Compliant System
IRQ 65536	Exclusive	Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 65536	Exclusive	Intel(R) Management Engine Interface
IRQ 65536	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
IRQ 65536	Exclusive	Intel(R) HD Graphics
IRQ 66	Exclusive	Microsoft ACPI-Compliant System
IRQ 67	Exclusive	Microsoft ACPI-Compliant System
IRQ 68	Exclusive	Microsoft ACPI-Compliant System
IRQ 69	Exclusive	Microsoft ACPI-Compliant System
IRQ 70	Exclusive	Microsoft ACPI-Compliant System
IRQ 71	Exclusive	Microsoft ACPI-Compliant System
IRQ 72	Exclusive	Microsoft ACPI-Compliant System
IRQ 73	Exclusive	Microsoft ACPI-Compliant System
IRQ 74	Exclusive	Microsoft ACPI-Compliant System
IRQ 75	Exclusive	Microsoft ACPI-Compliant System
IRQ 76	Exclusive	Microsoft ACPI-Compliant System
IRQ 77	Exclusive	Microsoft ACPI-Compliant System
IRQ 78	Exclusive	Microsoft ACPI-Compliant System
IRQ 79	Exclusive	Microsoft ACPI-Compliant System
IRQ 80	Exclusive	Microsoft ACPI-Compliant System
IRQ 81	Exclusive	Microsoft ACPI-Compliant System
IRQ 82	Exclusive	Microsoft ACPI-Compliant System
IRQ 83	Exclusive	Microsoft ACPI-Compliant System
IRQ 84	Exclusive	Microsoft ACPI-Compliant System
IRQ 85	Exclusive	Microsoft ACPI-Compliant System
IRQ 86	Exclusive	Microsoft ACPI-Compliant System
IRQ 87	Exclusive	Microsoft ACPI-Compliant System
IRQ 88	Exclusive	Microsoft ACPI-Compliant System
IRQ 89	Exclusive	Microsoft ACPI-Compliant System
IRQ 90	Exclusive	Microsoft ACPI-Compliant System
IRQ 91	Exclusive	Microsoft ACPI-Compliant System
IRQ 92	Exclusive	Microsoft ACPI-Compliant System
IRQ 93	Exclusive	Microsoft ACPI-Compliant System
IRQ 94	Exclusive	Microsoft ACPI-Compliant System
IRQ 95	Exclusive	Microsoft ACPI-Compliant System
IRQ 96	Exclusive	Microsoft ACPI-Compliant System
IRQ 97	Exclusive	Microsoft ACPI-Compliant System
IRQ 98	Exclusive	Microsoft ACPI-Compliant System
IRQ 99	Exclusive	Microsoft ACPI-Compliant System
Memory 000A0000-000BFFFF	Shared	PCI Express Root Complex
Memory 000A0000-000BFFFF	Shared	Intel(R) HD Graphics
Memory 000D0000-000D3FFF	Shared	PCI Express Root Complex
Memory 000D4000-000D7FFF	Shared	PCI Express Root Complex
Memory 000D8000-000DBFFF	Shared	PCI Express Root Complex
Memory 000DC000-000DFFFF	Shared	PCI Express Root Complex
Memory 000E0000-000E3FFF	Shared	PCI Express Root Complex
Memory 000E4000-000E7FFF	Shared	PCI Express Root Complex
Memory DFA00000-FEAFFFFF	Shared	PCI Express Root Complex
Memory E0000000-EFFFFFFF	Exclusive	Intel(R) HD Graphics
Memory F0000000-F0003FFF	Exclusive	Realtek PCIe GbE Family Controller
Memory F0000000-F00FFFFF	Exclusive	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12
Memory F0004000-F0004FFF	Exclusive	Realtek PCIe GbE Family Controller
Memory F7800000-F7BFFFFF	Exclusive	Intel(R) HD Graphics

Memory F7C00000-F7C0FFFF	Exclusive	Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
Memory F7C10000-F7C13FFF	Exclusive	High Definition Audio Controller
Memory F7C16000-F7C167FF	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Memory F7C17000-F7C173FF	Exclusive	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
Memory F7C18000-F7C183FF	Exclusive	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
Memory F7C1B000-F7C1B00F	Exclusive	Intel(R) Management Engine Interface
Port 0000-0CF7	Shared	PCI Express Root Complex
Port 0070-0077	Exclusive	System CMOS/real time clock
Port 0378-037F	Exclusive	Printer Port (LPT1)
Port 03B0-03BB	Shared	Intel(R) HD Graphics
Port 03C0-03DF	Shared	Intel(R) HD Graphics
Port 03F8-03FF	Exclusive	Communications Port (COM1)
Port 0D00-FFFF	Shared	PCI Express Root Complex
Port E000-E0FF	Exclusive	Realtek PCIe GbE Family Controller
Port E000-EFFF	Exclusive	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12
Port F000-F03F	Exclusive	Intel(R) HD Graphics
Port F060-F07F	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Port F080-F083	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Port F090-F097	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Port F0A0-F0A3	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02
Port F0B0-F0B7	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E02

Navigation

Input

[HID Keyboard Device]

Keyboard Properties:

Keyboard Name	HID Keyboard Device
Keyboard Type	IBM enhanced (101- or 102-key) keyboard
Keyboard Layout	US
ANSI Code Page	1252 - Western European (Windows)
OEM Code Page	437
Repeat Delay	1
Repeat Rate	31

[HID-compliant mouse]

Mouse Properties:

Mouse Name	HID-compliant mouse
Mouse Buttons	3
Mouse Hand	Right
Pointer Speed	1
Double-Click Time	500 msec
X/Y Threshold	6 / 10
Wheel Scroll Lines	3

Mouse Features:

Active Window Tracking	Disabled
ClickLock	Disabled
Hide Pointer While Typing	Enabled
Mouse Wheel	Present
Move Pointer To Default Button	Disabled

Pointer Trails	Disabled
Sonar	Disabled

Navigation

Printers

[Fax]

Printer Properties:

Printer Name	Fax
Default Printer	No
Share Point	Not shared
Printer Port	SHRFAX:
Printer Driver	Microsoft Shared Fax Driver (v4.00)
Device Name	Fax
Print Processor	winprint
Separator Page	None
Availability	8:00 AM - 8:00 AM
Priority	1
Print Jobs Queued	0
Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	200 x 200 dpi Mono

[Microsoft Print to PDF (Default)]

Printer Properties:

Printer Name	Microsoft Print to PDF
Default Printer	Yes
Share Point	Not shared
Printer Port	PORTPROMPT:
Printer Driver	Microsoft Print To PDF (v6.03)
Device Name	Microsoft Print to PDF
Print Processor	winprint
Separator Page	None
Availability	8:00 AM - 8:00 AM
Priority	1
Print Jobs Queued	0
Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	600 x 600 dpi Color

[Microsoft XPS Document Writer]

Printer Properties:

Printer Name	Microsoft XPS Document Writer
Default Printer	No

Share Point	Not shared
Printer Port	PORTPROMPT:
Printer Driver	Microsoft XPS Document Writer v4 (v6.03)
Device Name	Microsoft XPS Document Writer
Print Processor	winprint
Separator Page	None
Availability	8:00 AM - 8:00 AM
Priority	1
Print Jobs Queued	0
Status	Unknown

Navigation

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	600 x 600 dpi Color

[OneNote for Windows 10]

Printer Properties:

Printer Name	OneNote for Windows 10
Default Printer	No
Share Point	Not shared
Printer Port	Microsoft.Office.OneNote_16001.13127.20190.0_x64__8wekyb3d8bbwe_microsoft.onenoteim_S-1-5-21-233448718-3606551117-1202096394-1001
Printer Driver	Microsoft Software Printer Driver (v6.03)
Device Name	OneNote for Windows 10
Print Processor	winprint
Separator Page	None
Availability	Always
Priority	1
Print Jobs Queued	0
Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	300 x 300 dpi Color

[Send To OneNote 2016]

Printer Properties:

Printer Name	Send To OneNote 2016
Default Printer	No
Share Point	Not shared
Printer Port	nul:
Printer Driver	Send to Microsoft OneNote 16 Driver (v6.03)
Device Name	Send To OneNote 2016
Print Processor	winprint
Separator Page	None
Availability	Always
Priority	1
Print Jobs Queued	0
Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in

Orientation	Portrait
Print Quality	600 x 600 dpi Color

Navigation

Auto Start

Application Description	Start From	Application Command
AdobeAAMUpdater-1.0	Registry\Common\Run	C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe
Autodesk Desktop App	Registry\Common\Run	C:\Program Files (x86)\Autodesk\Autodesk Desktop App\AutodeskDesktopApp.exe -tray
Autodesk Genuine Service	Registry\Common\Run	C:\Users\bebos\AppData\Local\Programs\Autodesk\Genuine Service\GenuineService.exe
CsrAudioguiCtrl	Registry\Common\Run	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrAudioguiCtrl.exe
CSRHarmonySkypePlugin	Registry\Common\Run	C:\Program Files (x86)\CSR\CSR Harmony Wireless Software Stack\CSRHarmonySkypePlugin.exe
CsrHCRPServer	Registry\Common\Run	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrHCRPServer.exe
CsrSyncMLServer	Registry\Common\Run	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\CsrSyncMLServer.exe
HarmonyUserStartup	Registry\Common\Run	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\HarmonyUserStartup.exe
Krisp	Registry\User\Run	C:\Program Files\Krisp\Krisp.exe -s
MicrosoftEdgeAutoLaunch_6D63B0161E2DA57745AFDB4ECA13D212	Registry\User\Run	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe --no-startup-window /prefetch:5
OneDrive	Registry\User\Run	C:\Users\bebos\AppData\Local\Microsoft\OneDrive\OneDrive.exe /background
RTHDVCPL	Registry\Common\Run	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe -s
SecurityHealth	Registry\Common\Run	C:\WINDOWS\system32\SecurityHealthSystray.exe
SunJavaUpdateSched	Registry\Common\Run	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
TeamsMachineInstaller	Registry\Common\Run	C:\Program Files (x86)\Teams Installer\Teams.exe --checkInstall --source=PROPLUS
TrayApplication	Registry\Common\Run	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\TrayApplication.exe
vksts	Registry\Common\Run	C:\Program Files\CSR\CSR Harmony Wireless Software Stack\vksts.exe

Scheduled

[MicrosoftEdgeUpdateTaskMachineCore]

Task Properties:

Task Name	MicrosoftEdgeUpdateTaskMachineCore
Status	Enabled
Application Name	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
Application Parameters	/c
Working Folder	
Comment	Keeps your Microsoft software up to date. If this task is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Microsoft software using it.
Account Name	SYSTEM
Creator	
Last Run	9/12/2020 8:48:12 PM
Next Run	9/13/2020 11:26:34 AM

Task Triggers:

At log on	At log on of any user
Daily	At 11:26:34 AM every day

[MicrosoftEdgeUpdateTaskMachineUA]

Task Properties:

Navigation

Task Name	MicrosoftEdgeUpdateTaskMachineUA
Status	Enabled
Application Name	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
Application Parameters	/ua /installsource scheduler
Working Folder	
Comment	Keeps your Microsoft software up to date. If this task is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Microsoft software using it.
Account Name	SYSTEM
Creator	
Last Run	9/12/2020 8:48:10 PM
Next Run	9/12/2020 9:26:34 PM

Task Triggers:

Daily	At 11:26:34 AM every day - After triggered, repeat every 1 hour for a duration of 1 day

[OneDrive Standalone Update Task-S-1-5-21-233448718-3606551117-1202096394-1001]

Task Properties:

Task Name	OneDrive Standalone Update Task-S-1-5-21-233448718-3606551117-1202096394-1001
Status	Enabled
Application Name	%localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
Application Parameters	
Working Folder	
Comment	
Account Name	VIETHOANG\bebos
Creator	Microsoft Corporation
Last Run	9/12/2020 4:10:14 PM
Next Run	9/13/2020 4:49:10 PM

Task Triggers:

One time	At 2:00:00 PM on 5/1/1992 - After triggered, repeat every 1 day indefinitely

[Smart Clock]

Task Properties:

Task Name	Smart Clock
Status	Enabled
Application Name	C:\Users\bebos\AppData\Roaming\Smart Clock\SmartClock.exe
Application Parameters	
Working Folder	
Comment	
Account Name	VIETHOANG\bebos
Creator	
Last Run	9/12/2020 8:48:12 PM
Next Run	Unknown

Task Triggers:

At log on	At log on of any user

Installed Programs

Navigation

Program	Version	Inst. Size	GUID	Publisher	Inst. Date
ACA & [TRIAL VERSION]	8.3.51.0	Unknown	{28B89E [TRIAL VERSION]	Autodesk	2020-09-09
ACAD P [TRIAL VERSION]	24.0.47.0	Unknown	{28B89E [TRIAL VERSION]	Autodesk	2020-09-09
Adobe [TRIAL VERSION]	24.1.1	Unknown	ILST_24 [TRIAL VERSION]	Adobe Inc.	9/8/2020
Adobe [TRIAL VERSION]	9.2	Unknown	LTRM_9_ [TRIAL VERSION]	Adobe Inc.	9/8/2020
Adobe [TRIAL VERSION]	21.1.3	Unknown	PHSP_21 [TRIAL VERSION]	Adobe Inc.	9/8/2020
Adobe [TRIAL VERSION]	14.1	Unknown	PPRO_14 [TRIAL VERSION]	Adobe Inc.	9/8/2020
AIDA64 [TRIAL VERSION]	6.25	Unknown	AIDA64 [TRIAL VERSION]	FinalWire Ltd.	2020-09-12
AutoCA [TRIAL VERSION]	24.0.47.0	Unknown	{28B89E [TRIAL VERSION]	Autodesk	2020-09-09
AutoCA [TRIAL VERSION]	24.0.47.0	Unknown	{28B89E [TRIAL VERSION]	Autodesk	2020-09-09
AutoCA [TRIAL VERSION]	24.0.47.0	Unknown	{28B89E [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	3.1.0	Unknown	{DB92FE [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	24.0.47.0	Unknown	AutoCAD [TRIAL VERSION]	Autodesk	9/9/2020
Autode [TRIAL VERSION]	8.0.0.46	Unknown	Autodes [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	3.1.0	Unknown	{2CBD49 [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	3.2.18	Unknown	{54A006 [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	19.1.22.0	Unknown	{6774FD [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	19.1.22.0	Unknown	{6EFAD5 [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	3.0.26	Unknown	{A9005A [TRIAL VERSION]	Autodesk	2020-09-09
Autode [TRIAL VERSION]	11.2.0.1802	Unknown	{951BB0 [TRIAL VERSION]	Autodesk	2020-09-09
Chaos [TRIAL VERSION]	1.7.5	Unknown	Chaos C [TRIAL VERSION]	Chaos Software Ltd	
Chaos [TRIAL VERSION]	5.5.0	Unknown	Chaos L [TRIAL VERSION]	Chaos Software Ltd	
Chrome [TRIAL VERSION]	85.0.4183.6	Unknown	{044C96 [TRIAL VERSION]	Google Inc.	2020-09-09
Chrome [TRIAL VERSION]	1.0	Unknown	639e543 [TRIAL VERSION]	Chrome Remote Desktop	2020-09-09
CSR Ha [TRIAL VERSION]	2.1.63.0	Unknown	{17DEA0 [TRIAL VERSION]	Cambridge Silicon Radio Limited.	2020-09-09
Discord	0.0.308	Unknown	Discord	Discord Inc.	2020-05-12
iPadian version 10.1	10.1	Unknown	{31593709-9939-49BD-AA38-E74735EC43A4}_is1	iPadian	2020-09-12
Java 8 Update 261	8.0.2610.12	Unknown	{26A24AE4-039D-4CA4-87B4-2F32180261F0}	Oracle Corporation	2020-09-08
Java Auto Updater	2.8.261.12	Unknown	{4A03706F-666A-4037-7777-5F2748764D10}	Oracle Corporation	2020-09-08
Kartopolis	3.1	Unknown	Kartopolis	Palermont	
Krisp	1.18.8	Unknown	{ECB8AEDF-746C-4D35-BF7A-6BA02C7D289A}	Krisp Technologies, Inc	2020-09-09
Microsoft Edge Update	1.3.135.29	Unknown	Microsoft Edge Update		
Microsoft Edge	85.0.564.51	Unknown	Microsoft Edge	Microsoft Corporation	2020-09-11
Microsoft Office 365 ProPlus - en-us	16.0.12527.20988	Unknown	O365ProPlusRetail - en-us	Microsoft Corporation	
Microsoft OneDrive	20.143.0716.0003	Unknown	OneDriveSetup.exe	Microsoft Corporation	
Microsoft Teams	1.3.00.13565	Unknown	Teams	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219	Unknown	{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	Microsoft Corporation	2020-09-08
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	10.0.40219	Unknown	{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	Microsoft Corporation	2020-09-08
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030	11.0.61030.0	Unknown	{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	Microsoft Corporation	
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	11.0.61030.0	Unknown	{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	Microsoft Corporation	
Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030	11.0.61030	Unknown	{37B8F9C7-03FB-3253-8781-2517C99D7C00}	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030	11.0.61030	Unknown	{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030	11.0.61030	Unknown	{B175520C-86A2-35A7-8619-86DC379688B9}	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030	11.0.61030	Unknown	{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660	12.0.40660.0	Unknown	{ef6b00ec-13e1-4c25-9064-b2f383cb8412}	Microsoft Corporation	
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40660	12.0.40660.0	Unknown	{61087a79-ac85-455c-934d-1fa22cc64f36}	Microsoft Corporation	
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40660	12.0.40660	Unknown	{5740BD44-B58D-321A-AFC0-6D3D4556DD6C}	Microsoft Corporation	2020-09-08
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660	12.0.40660	Unknown	{CB0836EC-B072-368D-82B2-D3470BF95707}	Microsoft Corporation	2020-09-08
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40660	12.0.40660	Unknown	{7DAD0258-515C-3DD4-8964-BD714199E0F7}	Microsoft Corporation	2020-09-08
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40660	12.0.40660	Unknown	{E30D8B21-D82D-3211-82CC-0F0A5D1495E8}	Microsoft Corporation	2020-09-08
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.24.28127	14.24.28127.4	Unknown	{282975d8-55fe-4991-bbbb-06a72581ce58}	Microsoft Corporation	
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.24.28127	14.24.28127.4	Unknown	{e31cb1a4-76b5-46a5-a084-3fa419e82201}	Microsoft Corporation	

Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127	14.24.28127	Unknown	{8678BA04-D161-45BE-ACA4-CC5D13073I	Navigation -ation	2020-09-09
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127	14.24.28127	Unknown	{7DC387B8-E6A2-480C-8EF9-A6E51AE81C19}	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127	14.24.28127	Unknown	{EAC73207-74BD-4B13-AACF-8C0E751FA4E8}	Microsoft Corporation	2020-09-09
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127	14.24.28127	Unknown	{2E72FA1F-BADB-4337-B8AE-F7C17EC57D1D}	Microsoft Corporation	2020-09-09
Minecraft Launcher	1.0.0.0	Unknown	{F6678473-0198-46D0-A88F-2A247E6FA03C}	Mojang	2020-09-08
Notepad++ (32-bit x86)	7.8.8	Unknown	Notepad++	Notepad++ Team	
Office 16 Click-to-Run Extensibility Component 64-bit Registration	16.0.12527.20988	Unknown	{90160000-00DD-0000-1000-0000000FF1CE}	Microsoft Corporation	2020-09-09
Office 16 Click-to-Run Extensibility Component	16.0.12527.20988	Unknown	{90160000-008C-0000-0000-0000000FF1CE}	Microsoft Corporation	2020-09-09
Office 16 Click-to-Run Licensing Component	16.0.12527.20988	Unknown	{90160000-008F-0000-1000-0000000FF1CE}	Microsoft Corporation	2020-09-09
Office 16 Click-to-Run Localization Component	16.0.12527.20988	Unknown	{90160000-008C-0409-0000-0000000FF1CE}	Microsoft Corporation	2020-09-09
Realtek High Definition Audio Driver	6.0.8746.1	Unknown	{F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}	Realtek Semiconductor Corp.	
SketchUp 2020	20.2.172	Unknown	{522800F1-9FCE-44F2-8D2E-2CEC5B25A9C2}	Trimble, Inc.	
SketchUpPro	20.2.172.37	Unknown	{5778f9a3-781e-16f1-a6bf-08fd59dfa77b}	SketchUp	2020-09-09
Teams Machine-Wide Installer	1.3.0.13565	Unknown	{39AF0813-FA7B-4860-ADBE-93B9B214B914}	Microsoft Corporation	2020-09-09
Univer [TRIAL VERSION]	1.7.1	Unknown	{86633C [TRIAL VERSION]	oPryzeLP	2020-09-08
V-Ray [TRIAL VERSION]	4.20.03	Unknown	V-Ray f [TRIAL VERSION]	Chaos Software Ltd	
V-Ray [TRIAL VERSION]	1.4.4	Unknown	V-Ray S [TRIAL VERSION]	Chaos Software Ltd	
Window [TRIAL VERSION]	1.4.9200.23072	Unknown	{D5C697 [TRIAL VERSION]	Microsoft Corporation	
WinRAR [TRIAL VERSION]	5.91.0	Unknown	WinRAR [TRIAL VERSION]	win.rar GmbH	
WO Mic [TRIAL VERSION]		Unknown	WOMic [TRIAL VERSION]		
Wold [TRIAL VERSION]	2.9	Unknown	Wold [TRIAL VERSION]	Kaferolsd	

Licenses

Software	Product Key
Autodesk AutoCAD 2021 - English	000-00 [TRIAL VERSION]
Microsoft Internet Explorer 11.508.19041.0	VK7JG- [TRIAL VERSION]
Microsoft Windows 10 Pro	VK7JG- [TRIAL VERSION]

File Types

Extension	File Type Description	Content Type
001	WinRAR archive	
386	Virtual Device Driver	
7Z	WinRAR archive	
8BA	8BA File	
8BC	8BC File	
8BE	8BE File	
8BF	Adobe Photoshop Plugin	
8BI	Adobe Photoshop Plugin	
8BP	8BP File	
8BS	8BS File	
8BX	8BX File	
8BY	8BY File	
8LI	8LI File	
ABR	ABR File	
ACBL	Adobe Color Book File	
ACCDA	Microsoft Access Add-in	application/msaccess.addin
ACCDB	Microsoft Access Database	application/msaccess
ACCDC	Microsoft Access Signed Package	application/msaccess.cab

ACCDE	Microsoft Access ACCDE Database	application/msaccess.exec
ACCDR	Microsoft Access Runtime Application	application/msaccess.runtime
ACCDT	Microsoft Access Template	application/msaccess.template
ACCDU	Microsoft Access Add-in Data	
ACCDW	Microsoft Access Web Application	application/msaccess.webapplication
ACCFT	Microsoft Access Template	application/msaccess.ftemplate
ACCOUNTPICTURE-MS	Account Picture File	application/windows-accountpicture
ACF	ACF File	
ACL	AutoCorrect List File	
ACO	ACO File	
ACT	ACT File	
ACV	ACV File	
ADE	Microsoft Access Project Extension	application/msaccess
ADN	Microsoft Access Blank Project Template	
ADO	ADO File	
ADP	Microsoft Access Project	application/msaccess
AEX	Adobe PremierePro Effect	
AHS	AHS File	
AHU	AHU File	
AI	Adobe Illustrator Artwork 24.0	application/postscript
AIA	Adobe Illustrator Action File	
AIP	Adobe Illustrator Plugin	
AIT	Adobe Illustrator Template	
ALV	ALV File	
AMP	AMP File	
AMS	AMS File	
ANI	Animated Cursor	
API	API File	
APK	APK File	
APL	APL File	
APPCONTENT-MS	Application Content	application/windows-appcontent+xml
APPLICATION	Application Manifest	application/x-ms-application
APPREF-MS	Application Reference	
ARJ	WinRAR archive	
ASA	ASA File	
ASE	Adobe Illustrator Swatch Exchange File	
ASL	ASL File	
ASP	ASP File	
AST	AST File	
ASV	ASV File	
ATF	ATF File	
ATN	ATN File	
AVA	AVA File	
AW	Answer Wizard File	
AXT	AXT File	
BAT	Windows Batch File	
BLG	Performance Monitor File	
BLW	BLW File	
BMP	Bitmap Image	image/bmp
BZ	WinRAR archive	
BZ2	WinRAR archive	
CAB	WinRAR archive	
CAMP	WCS Viewing Condition Profile	
CAT	Security Catalog	application/vnd.ms-pki.seccat
CDMP	WCS Device Profile	

Navigation

Navigation

CDX	CDX File	
CDXML	CDXML File	
CER	Security Certificate	application/x-x509-ca-cert
CHA	CHA File	
CHK	Recovered File Fragments	
CHM	Compiled HTML Help file	
CIN	CIN File	
CMD	Windows Command Script	
COM	MS-DOS Application	
COMPOSITEFONT	Composite Font File	
CPL	Control Panel Item	
CRL	Certificate Revocation List	application/pkix-crl
CRT	Security Certificate	application/x-x509-ca-cert
CRTX	Microsoft Office Chart Template	
CSF	Adobe Color Settings File	
CSH	CSH File	
CSRBTSENDTOCLASS	CSRSendToShellExt Class	
CSS	Cascading Style Sheet Document	text/css
CSV	Microsoft Excel Comma Separated Values File	application/vnd.ms-excel
CUR	Cursor	
DAE	DAE File	
DB	Data Base File	
DCM	Adobe Photoshop DCMFileType.140	
DCP	DCP File	
DCPR	DCPR File	
DCTX	Open Extended Dictionary	
DCTXC	Open Extended Dictionary	
DDS	DDS Image	image/vnd.ms-dds
DEL	Adobe Premiere Edit Decision List	
DER	Security Certificate	application/x-x509-ca-cert
DESKLINK	Desktop Shortcut	
DESKTHEMEPACK	Windows Desktop Theme Pack	
DET	Office Data File	
DIAGCAB	Diagnostic Cabinet	
DIAGCFG	Diagnostic Configuration	
DIAGPKG	Diagnostic Document	
DIB	Bitmap Image	image/bmp
DIC	DIC File	
DLL	Application Extension	application/x-msdownload
DLX	Adobe Premiere Movie	
DOC	Microsoft Word 97 - 2003 Document	application/msword
DOCHTML	Microsoft Word HTML Document	
DOCM	Microsoft Word Macro-Enabled Document	application/vnd.ms-word.document.macroEnabled.12
DOCMHTML	DOCMHTML File	
DOCX	Microsoft Word Document	application/vnd.openxmlformats-officedocument.wordprocessingml.document
DOCXML	Microsoft Word XML Document	
DOT	Microsoft Word 97 - 2003 Template	application/msword
DOTHTML	Microsoft Word HTML Template	
DOTM	Microsoft Word Macro-Enabled Template	application/vnd.ms-word.template.macroEnabled.12
DOTX	Microsoft Word Template	application/vnd.openxmlformats-officedocument.wordprocessingml.template
DQY	Microsoft Excel ODBC Query File	
DRV	Device Driver	
DSN	Microsoft OLE DB Provider for ODBC Drivers	
EAP	EAP File	
ELM	Microsoft Office Themes File	

EMF	EMF File	image/x-emf
EML	E-mail Message	
EPR	EPR File	
EVT	EVT File	
EVTX	EVTX File	
EXC	EXC File	
EXE	Application	application/x-msdownload
EXR	EXR File	
FDM	Outlook Form Definition	
FFO	FFO File	
FL3	FL3 File	
FLT	Adobe Illustrator Filter	
FON	Font file	
FXG	FXG File	
GCSX	Microsoft Office SmartArt Graphic Color Variation	
GIF	GIF Image	image/gif
GLOX	Microsoft Office SmartArt Graphic Layout	
GMMP	WCS Gamut Mapping Profile	
GQSX	Microsoft Office SmartArt Graphic Quick Style	
GRA	Microsoft Graph Chart	
GRD	GRD File	
GRP	Microsoft Program Group	
GZ	WinRAR archive	application/x-gzip
HDR	HDR File	
HLP	Help File	
HOL	Outlook Holidays	
HTA	HTML Application	application/hta
HTM	HTML Document	text/html
HTML	HTML Document	text/html
HXA	Microsoft Help Attribute Definition File	application/xml
HXC	Microsoft Help Collection Definition File	application/xml
HXD	Microsoft Help Validator File	application/octet-stream
HXE	Microsoft Help Samples Definition File	application/xml
HXF	Microsoft Help Include File	application/xml
HXH	Microsoft Help Merged Hierarchy File	application/octet-stream
HXI	Microsoft Help Compiled Index File	application/octet-stream
HXK	Microsoft Help Index File	application/xml
HXQ	Microsoft Help Merged Query Index File	application/octet-stream
HXR	Microsoft Help Merged Attribute Index File	application/octet-stream
HXS	Microsoft Help Compiled Storage File	application/octet-stream
HXT	Microsoft Help Table of Contents File	application/xml
HXV	Microsoft Help Virtual Topic Definition File	application/xml
HXW	Microsoft Help Attribute Definition File	application/octet-stream
HYP	Adobe Illustrator Hyphenation Dictionary	
ICC	ICC Profile	
ICL	Icon Library	
ICM	ICC Profile	
ICO	Icon	image/x-icon
ICS	iCalendar File	text/calendar
IDEA	IDEA File	
IFF	Adobe Photoshop IFFFileType.140	
IGP	Intel Graphics Profiles	
IMESX	IME Search provider definition	
IMG	Disc Image File	
IQY	Microsoft Excel Web Query File	text/x-ms-iqy

Navigation

IROS	IROS File	
IRS	IRS File	
ISO	WinRAR archive	
JAR	Executable Jar File	
JFIF	JPEG Image	image/jpeg
JNLP	JNLP File	application/x-java-jnlp-file
JOB	Task Scheduler Task Object	
JOD	Microsoft.Jet.OLEDB.4.0	
JPE	JPEG Image	image/jpeg
JPEG	JPEG Image	image/jpeg
JPG	JPEG Image	image/jpeg
JPS	Adobe Photoshop JPSFileType.140	
JS	JavaScript File	
JSE	JScript Encoded File	
JXR	Windows Media Photo	image/vnd.ms-photo
KMZ	KMZ File	
KYS	KYS File	
LABEL	Property List	
LACCDB	Microsoft Access Record-Locking Information	
LAYOUT	Adobe Premiere Layout	
LDB	Microsoft Access Record-Locking Information	
LEX	Dictionary File	
LHA	WinRAR archive	
LIBRARY-MS	Library Folder	application/windows-library+xml
LNK	Shortcut	
LRCAT	Adobe Lightroom Classic	
LZ	WinRAR archive	
LZH	WinRAR archive	
MAD	Microsoft Access Module Shortcut	
MAF	Microsoft Access Form Shortcut	
MAG	Microsoft Access Diagram Shortcut	
MAM	Microsoft Access Macro Shortcut	
MAPIMAIL	Mail Service	
MAQ	Microsoft Access Query Shortcut	
MAR	Microsoft Access Report Shortcut	
MAS	Microsoft Access Stored Procedure Shortcut	
MAT	Microsoft Access Table Shortcut	
MAU	MAU File	
MAV	Microsoft Access View Shortcut	
MAW	Microsoft Access Data Access Page Shortcut	
MDA	Microsoft Access Add-in	application/msaccess
MDB	Microsoft Access Database	application/msaccess
MDBHTML	Microsoft Access HTML Document	
MDE	Microsoft Access MDE Database	application/msaccess
MDN	Microsoft Access Blank Database Template	
MDT	Microsoft Access Add-in Data	
MDW	Microsoft Access Workgroup Information	
MFW	MFW File	
MHT	MHTML Document	message/rfc822
MHTML	MHTML Document	message/rfc822
MLC	Language Pack File_	
MSC	Microsoft Common Console Document	
MSG	Outlook Item	
MSI	Windows Installer Package	
MSP	Windows Installer Patch	

Navigation

MSRCINCIDENT	Windows Remote Assistance Invitation	
MSSTYLES	Windows Visual Style File	
MSU	Microsoft Update Standalone Package	
MS-WINDOWS-STORE-LICENSE	Windows Store License	
MTL	MTL File	
MYDOCS	MyDocs Drop Target	
NFO	MSInfo Configuration File	
NK2	Outlook Nickname File	
NST	Outlook Data File	
OCX	ActiveX control	
ODC	Microsoft Office Data Connection	text/x-ms-odc
ODCCUBEFILE	ODCCUBEFILE File	
ODCDATABASEFILE	ODCDATABASEFILE File	
ODCNEWFILE	ODCNEWFILE File	
ODCTABLECOLLECTIONFILE	ODCTABLECOLLECTIONFILE File	
ODCTABLEFILE	ODCTABLEFILE File	
ODP	OpenDocument Presentation	application/vnd.oasis.opendocument.presentation
ODS	OpenDocument Spreadsheet	application/vnd.oasis.opendocument.spreadsheet
ODT	OpenDocument Text	application/vnd.oasis.opendocument.text
OFS	Outlook Form Regions	
OFT	Outlook Item Template	
OLS	Office List Shortcut	application/vnd.ms-publisher
ONE	Microsoft OneNote Section	application/msonenote
ONEPKG	Microsoft OneNote Single File Package	application/msonenote
ONETOC	Microsoft OneNote 2003 Table Of Contents	
ONETOC2	Microsoft OneNote Table Of Contents	
OPC	Microsoft Clean-up Wizard File	
OQY	Microsoft Excel OLAP Query File	
OSDX	OpenSearch Description File	application/opensearchdescription+xml
OST	Outlook Data File	
OTF	OpenType Font file	
OTM	Outlook VBA Project File	
P10	Certificate Request	application/pkcs10
P12	Personal Information Exchange	application/x-pkcs12
P3L	P3L File	
P3M	P3M File	
P3R	P3R File	
P7B	PKCS #7 Certificates	application/x-pkcs7-certificates
P7C	Digital ID File	application/pkcs7-mime
P7M	PKCS #7 MIME Message	application/pkcs7-mime
P7R	Certificate Request Response	application/x-pkcs7-certreqresp
P7S	PKCS #7 Signature	application/pkcs7-signature
PAB	Outlook Personal Address Book	
PARTIAL	Partial Download	
PBK	Dial-Up Phonebook	
PBM	PBM File	
PCB	PCB File	
PCD	PCD File	
PCX	PCX File	
PDD	PDD File	
PDP	PDP File	
PERFMONCFG	Performance Monitor Configuration	
PFM	Type 1 Font file	
PFX	Personal Information Exchange	application/x-pkcs12
PIF	Shortcut to MS-DOS Program	

PKO	Public Key Security Object	application/vnd.ms-pki.pko
PLE	PLE File	
PNF	Precompiled Setup Information	
PNG	PNG Image	image/png
POT	Microsoft PowerPoint 97-2003 Template	application/vnd.ms-powerpoint
POTHTML	Microsoft PowerPoint HTML Template	
POTM	Microsoft PowerPoint Macro-Enabled Design Template	application/vnd.ms-powerpoint.template.macroEnabled.12
POTX	Microsoft PowerPoint Template	application/vnd.openxmlformats-officedocument.presentationml.template
PPA	Microsoft PowerPoint 97-2003 Addin	application/vnd.ms-powerpoint
PPAM	Microsoft PowerPoint Addin	application/vnd.ms-powerpoint.addin.macroEnabled.12
PPJ	Adobe Premiere Project	
PPKG	RunTime Provisioning Tool	
PPROJ	Adobe Premiere Project	
PPS	Microsoft PowerPoint 97-2003 Slide Show	application/vnd.ms-powerpoint
PPSM	Microsoft PowerPoint Macro-Enabled Slide Show	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
PPSX	Microsoft PowerPoint Slide Show	application/vnd.openxmlformats-officedocument.presentationml.slideshow
PPT	Microsoft PowerPoint 97-2003 Presentation	application/vnd.ms-powerpoint
PPTHTML	Microsoft PowerPoint HTML Document	
PPTM	Microsoft PowerPoint Macro-Enabled Presentation	application/vnd.ms-powerpoint.presentation.macroEnabled.12
PPTMHTML	PPTMHTML File	
PPTX	Microsoft PowerPoint Presentation	application/vnd.openxmlformats-officedocument.presentationml.presentation
PPTXML	Microsoft PowerPoint XML Presentation	
PREXPORT	PREXPORT File	
PRF	PICS Rules File	application/pics-rules
PRFPSET	PRFPSET File	
PRINTEREXPORT	Printer Migration File	
PRM	Adobe Premiere Plugin	
PRMP	Adobe Premiere Plugin	
PRPRESET	PRPRESET File	
PRPROJ	Adobe Premiere Project	
PRSL	PRSL File	
PRTL	Adobe Premiere Title	
PS1XML	PS1XML File	
PSB	PSB File	
PSC1	PSC1 File	application/PowerShell
PSD	Adobe Photoshop Image.21	
PSDT	PSDT File	
PSP	PSP File	
PSSC	PSSC File	
PST	Outlook Data File	
PUB	Microsoft Publisher Document	application/vnd.ms-publisher
PUBHTML	PUBHTML File	
PUBMHTML	PUBMHTML File	
PWZ	Microsoft PowerPoint Wizard	application/vnd.ms-powerpoint
PXR	PXR File	
QDS	Directory Query	
R00	WinRAR archive	
R01	WinRAR archive	
R02	WinRAR archive	
R03	WinRAR archive	
R04	WinRAR archive	
R05	WinRAR archive	
R06	WinRAR archive	
R07	WinRAR archive	
R08	WinRAR archive	

Navigation

R09	WinRAR archive	
R10	WinRAR archive	
R11	WinRAR archive	
R12	WinRAR archive	
R13	WinRAR archive	
R14	WinRAR archive	
R15	WinRAR archive	
R16	WinRAR archive	
R17	WinRAR archive	
R18	WinRAR archive	
R19	WinRAR archive	
R20	WinRAR archive	
R21	WinRAR archive	
R22	WinRAR archive	
R23	WinRAR archive	
R24	WinRAR archive	
R25	WinRAR archive	
R26	WinRAR archive	
R27	WinRAR archive	
R28	WinRAR archive	
R29	WinRAR archive	
RAR	WinRAR archive	
RAT	Rating System File	application/rat-file
RDP	Remote Desktop Connection	
REG	Registration Entries	
RELS	XML Document	
RESMONCFG	Resource Monitor Configuration	
REV	RAR recovery volume	
RLE	RLE File	
RLL	Application Extension	
RQY	Microsoft Excel OLE DB Query File	text/x-ms-rqy
RTF	Rich Text Format	application/msword
SBX	Adobe Illustrator Tsume File	
SCF	File Explorer Command	
SCR	Screen saver	
SCT	SCT File	text/scriptlet
SEARCHCONNECTOR-MS	Search Connector Folder	application/windows-search-connector+xml
SEARCH-MS	Saved Search	
SETTINGCONTENT-MS	Setting Content	
SFCACHE	ReadyBoost Cache File	
SHC	SHC File	
SHH	SHH File	
SKM	SketchUp File	
SKP	SketchUp File	
SLDM	Microsoft PowerPoint Macro-Enabled Slide	application/vnd.ms-powerpoint.slide.macroEnabled.12
SLDX	Microsoft PowerPoint Slide	application/vnd.openxmlformats-officedocument.presentationml.slide
SLK	Microsoft Excel SLK Data Import Format	application/vnd.ms-excel
SMRD	Adobe Illustrator Filter	
SPC	PKCS #7 Certificates	application/x-pkcs7-certificates
SPL	Shockwave Flash Object	application/futuresplash
SST	Microsoft Serialized Certificate Store	application/vnd.ms-pki.certstore
STA	STA File	
STYLE	Style Builder File	
SVG	SVG Document	image/svg+xml
SWF	Shockwave Flash Object	application/x-shockwave-flash

Navigation

SYMLINK	.symlink	
SYS	System file	
TAR	WinRAR archive	application/x-tar
TAZ	WinRAR archive	
TBZ	WinRAR archive	
TBZ2	WinRAR archive	
TGA	TGA File	
TGZ	WinRAR archive	application/x-compressed
THEME	Windows Theme File	
THEMEPACK	Windows Theme Pack	
THMX	Microsoft Office Theme	application/vnd.ms-officetheme
TIF	TIF File	image/tiff
TIFF	TIFF File	image/tiff
TLZ	WinRAR archive	
TPL	TPL File	
TTC	TrueType Collection Font file	
TTF	TrueType Font file	
TXZ	WinRAR archive	
U3D	U3D File	
UDL	Microsoft Data Link	
URL	URL File	
UU	WinRAR archive	
UUE	WinRAR archive	
UXDC	UXDC File	
VBE	VBScript Encoded File	
VBS	VBScript Script File	
VCF	vCard File	text/x-vcard
VCS	vCalendar File	
VDW	Microsoft Visio Document	application/vnd.ms-visio.viewer
VDX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VHD	Disc Image File	
VHDPMEM	Disc Image File	
VHDX	Disc Image File	
VPR	VPR File	
VSD	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSDM	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSDX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSS	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSSM	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSSX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VST	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSTM	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSTO	VSTO Deployment Manifest	application/x-ms-vsto
VSTX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VTX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VXD	Virtual Device Driver	
WAB	Address Book File	
WBCAT	Windows Backup Catalog File	
WBK	Microsoft Word Backup Document	application/msword
WCX	Workspace Configuration File	
WDP	Windows Media Photo	image/vnd.ms-photo
WEBPNP	Web Point And Print File	
WEBSITE	Pinned Site Shortcut	application/x-mswebsite
WIN	WIN File	

WIZ	Microsoft Word Wizard	application/msword
WIZHTML	Microsoft Access HTML Template	
WLL	WLL File	
WMF	WMF File	image/x-wmf
WSC	Windows Script Component	text/scriptlet
WSF	Windows Script File	
WSH	Windows Script Host Settings File	
XAML	Windows Markup File	application/xaml+xml
XAPK	XAPK File	
XBAP	XAML Browser Application	application/x-ms-xbap
XEVGENXML	XEVGENXML File	
XHT	XHTML Document	application/xhtml+xml
XHTML	XHTML Document	application/xhtml+xml
XLA	Microsoft Excel Add-In	application/vnd.ms-excel
XLAM	Microsoft Excel Add-In	application/vnd.ms-excel.addin.macroEnabled.12
XLD	Microsoft Excel 5.0 DialogSheet	application/vnd.ms-excel
XLK	Microsoft Excel Backup File	application/vnd.ms-excel
XLL	Microsoft Excel XLL Add-In	application/vnd.ms-excel
XLM	Microsoft Excel 4.0 Macro	application/vnd.ms-excel
XLS	Microsoft Excel 97-2003 Worksheet	application/vnd.ms-excel
XLSB	Microsoft Excel Binary Worksheet	application/vnd.ms-excel.sheet.binary.macroEnabled.12
XLSHTML	Microsoft Excel HTML Document	
XLSM	Microsoft Excel Macro-Enabled Worksheet	application/vnd.ms-excel.sheet.macroEnabled.12
XLSMHTML	XLSMHTML File	
XLSX	Microsoft Excel Worksheet	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
XLT	Microsoft Excel Template	application/vnd.ms-excel
XLTHTML	Microsoft Excel HTML Template	
XLTM	Microsoft Excel Macro-Enabled Template	application/vnd.ms-excel.template.macroEnabled.12
XLTX	Microsoft Excel Template	application/vnd.openxmlformats-officedocument.spreadsheetml.template
XLW	Microsoft Excel Workspace	application/vnd.ms-excel
XLXML	Microsoft Excel XML Worksheet	
XML	XML Document	text/xml
XRM-MS	XrML Digital License	text/xml
XSL	XSL Stylesheet	text/xml
XXE	WinRAR archive	
XZ	WinRAR archive	
Z	WinRAR archive	application/x-compress
ZFSENDTOTARGET	Compressed (zipped) Folder SendTo Target	
ZIP	WinRAR ZIP archive	application/x-zip-compressed
ZIPX	WinRAR archive	

Navigation

Windows Security

Operating System Properties:

OS Name	Microsoft Windows 10 Pro
OS Service Pack	[TRIAL VERSION]
Winlogon Shell	explorer.exe
User Account Control (UAC)	Enabled
UAC Remote Restrictions	Enabled
System Restore	Enabled
Windows Update Agent	10.0.19041.1 (WinBuild.160101.0800)

Data Execution Prevention (DEP, NX, EDB):

Supported by Operating System	Yes
Supported by CPU	Yes
Active (To Protect Applications)	Yes
Active (To Protect Drivers)	Yes

Navigation

Windows Update

Update Description	Update Type	Inst. Date
(Automatic Update)	Unknown	
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.737.0)	Update	9/9/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.742.0)	Update	9/9/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.817.0)	Update	9/9/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.819.0)	Update	9/9/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.862.0)	Update	9/10/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.870.0)	Update	9/10/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.910.0)	Update	9/11/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.941.0)	Update	9/11/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.984.0)	Update	9/12/2020
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.999.0)	Update	9/12/2020
Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2008.9)	Update	9/9/2020
Windows Malicious Software Removal Tool x64 - v5.82 (KB890830)	Update	9/9/2020

Anti-Virus

Software Description	Software Version	Virus Database Date	Known Viruses
Windows Defender	4.18.2008.9	9/12/2020	?

Firewall

Software Description	Software Version	Status
Windows Firewall	10.0.19041.1	Enabled

Anti-Spyware

Software Description	Software Version
Microsoft Windows Defender	4.18.2008.9

Regional

Time Zone:

Current Time Zone	SE Asia Standard Time
Current Time Zone Description	(UTC+07:00) Bangkok, Hanoi, Jakarta

Change To Standard Time
Change To Daylight Saving Time

Navigation

Language:

Language Name (Native)	English
Language Name (English)	English
Language Name (ISO 639)	en

Country/Region:

Country Name (Native)	United States
Country Name (English)	United States
Country Name (ISO 3166)	US
Country Code	1

Currency:

Currency Name (Native)	US Dollar
Currency Name (English)	US Dollar
Currency Symbol (Native)	$
Currency Symbol (ISO 4217)	USD
Currency Format	$123,456,789.00
Negative Currency Format	($123,456,789.00)

Formatting:

Time Format	h:mm:ss tt
Short Date Format	M/d/yyyy
Long Date Format	dddd, MMMM d, yyyy
Number Format	123,456,789.00
Negative Number Format	-123,456,789.00
List Format	first, second, third
Native Digits	0123456789

Days of Week:

Native Name for Monday	Monday / Mon
Native Name for Tuesday	Tuesday / Tue
Native Name for Wednesday	Wednesday / Wed
Native Name for Thursday	Thursday / Thu
Native Name for Friday	Friday / Fri
Native Name for Saturday	Saturday / Sat
Native Name for Sunday	Sunday / Sun

Months:

Native Name for January	January / Jan
Native Name for February	February / Feb
Native Name for March	March / Mar
Native Name for April	April / Apr
Native Name for May	May / May
Native Name for June	June / Jun
Native Name for July	July / Jul
Native Name for August	August / Aug
Native Name for September	September / Sep
Native Name for October	October / Oct
Native Name for November	November / Nov
Native Name for December	December / Dec

Miscellaneous:

Calendar Type	Gregorian (localized)
Default Paper Size	US Letter
Measurement System	U.S.

Display Languages:

LCID 0409h (Active)	English (United States)
LCID 042Ah	Vietnamese (Vietnam)

Navigation

Environment

Variable	Value
__COMPAT_LAYER	DetectorsAppHealth
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Users\bebos\AppData\Roaming
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramFiles	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	VIETHOANG
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
FPS_BROWSER_APP_PROFILE_STRING	Internet Explorer
FPS_BROWSER_USER_PROFILE_STRING	Default
HOMEDRIVE	C:
HOMEPATH	\Users\bebos
LOCALAPPDATA	C:\Users\bebos\AppData\Local
LOGONSERVER	\\VIETHOANG
NUMBER_OF_PROCESSORS	4
OneDrive	C:\Users\bebos\OneDrive
OneDriveConsumer	C:\Users\bebos\OneDrive
OS	Windows_NT
Path	C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\Op
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_ARCHITEW6432	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 58 Stepping 9, GenuineIntel
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	3a09
ProgramData	C:\ProgramData
ProgramFiles(x86)	C:\Program Files (x86)
ProgramFiles	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	C:\Program Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
PUBLIC	C:\Users\Public
SystemDrive	C:
SystemRoot	C:\WINDOWS
TEMP	C:\Users\bebos\AppData\Local\Temp
TMP	C:\Users\bebos\AppData\Local\Temp
USERDOMAIN_ROAMINGPROFILE	VIETHOANG
USERDOMAIN	VIETHOANG
USERNAME	bebos
USERPROFILE	C:\Users\bebos
windir	C:\WINDOWS

Navigation

Control Panel

Name	Comment
Flash Player	Manage Flash Player Settings
Java	Java Control Panel

Recycle Bin

Drive	Items Size	Items Count	Space %	Recycle Bin
C:	0	1	?	?

System Files

[system.ini]

```
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
```

[win.ini]

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

[hosts]

```
0.0.0.0 adclick.g.doublecklick.net
0.0.0.0 adeventtracker.spotify.com
0.0.0.0 ads-fa.spotify.com
0.0.0.0 analytics.spotify.com
0.0.0.0 audio2.spotify.com
0.0.0.0 b.scorecardresearch.com
```

Navigation

0.0.0.0 bounceexchange.com
0.0.0.0 bs.serving-sys.com
0.0.0.0 content.bitsontherun.com
0.0.0.0 core.insightexpressai.com
0.0.0.0 crashdump.spotify.com
0.0.0.0 d2gi7ultltnc2u.cloudfront.net
0.0.0.0 d3rt1990lpmkn.cloudfront.net
0.0.0.0 desktop.spotify.com
0.0.0.0 doubleclick.net
0.0.0.0 ds.serving-sys.com
0.0.0.0 googleadservices.com
0.0.0.0 googleads.g.doubleclick.net
0.0.0.0 gtssl2-ocsp.geotrust.com
0.0.0.0 js.moatads.com
0.0.0.0 log.spotify.com
0.0.0.0 media-match.com
0.0.0.0 omaze.com
0.0.0.0 pagead46.l.doubleclick.net
0.0.0.0 pagead2.googlesyndication.com
0.0.0.0 partner.googleadservices.com
0.0.0.0 pubads.g.doubleclick.net
0.0.0.0 redirector.gvt1.com
0.0.0.0 s0.2mdn.net
0.0.0.0 securepubads.g.doubleclick.net
0.0.0.0 tpc.googlesyndication.com
0.0.0.0 v.jwpcdn.com
0.0.0.0 video-ad-stats.googlesyndication.com
0.0.0.0 weblb-wg.gslb.spotify.com
0.0.0.0 www.googleadservices.com
0.0.0.0 www.googletagservices.com
0.0.0.0 www.omaze.com

[lmhosts.sam]

System Folders

System Folder	Path
Administrative Tools	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools
AppData	C:\Users\bebos\AppData\Roaming
Cache	C:\Users\bebos\AppData\Local\Microsoft\Windows\INetCache
CD Burning	C:\Users\bebos\AppData\Local\Microsoft\Windows\Burn\Burn
Common Administrative Tools	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools
Common AppData	C:\ProgramData
Common Desktop	C:\Users\Public\Desktop
Common Documents	C:\Users\Public\Documents
Common Favorites	C:\Users\bebos\Favorites
Common Files (x86)	C:\Program Files (x86)\Common Files
Common Files	C:\Program Files\Common Files
Common Music	C:\Users\Public\Music
Common Pictures	C:\Users\Public\Pictures
Common Programs	C:\ProgramData\Microsoft\Windows\Start Menu\Programs

Navigation

Common Start Menu	C:\ProgramData\Microsoft\Windows\Start Menu
Common Startup	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Common Templates	C:\ProgramData\Microsoft\Windows\Templates
Common Video	C:\Users\Public\Videos
Cookies	C:\Users\bebos\AppData\Local\Microsoft\Windows\INetCookies
Desktop	C:\Users\bebos\Desktop
Device	C:\WINDOWS\inf
Favorites	C:\Users\bebos\Favorites
Fonts	C:\WINDOWS\Fonts
History	C:\Users\bebos\AppData\Local\Microsoft\Windows\History
Local AppData	C:\Users\bebos\AppData\Local
My Documents	C:\Users\bebos\Documents
My Music	C:\Users\bebos\Music
My Pictures	C:\Users\bebos\Pictures
My Video	C:\Users\bebos\Videos
NetHood	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Network Shortcuts
PrintHood	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
Profile	C:\Users\bebos
Program Files (x86)	C:\Program Files (x86)
Program Files	C:\Program Files
Programs	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Recent	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Recent
Resources	C:\WINDOWS\resources
SendTo	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Start Menu
Startup	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
System (x86)	C:\WINDOWS\SysWOW64
System	C:\WINDOWS\system32
Temp	C:\Users\bebos\AppData\Local\Temp\
Templates	C:\Users\bebos\AppData\Roaming\Microsoft\Windows\Templates
Windows	C:\WINDOWS

Event Logs

Log Name	Event Type	Category	Generated On	User	Source	Description
Application	Warning	1	2020-09-08 11:54:26		ESENT	642: svchost (2908,D,35) SRUJet: The database format feature version 9180 (0x23dc) could not be used due to the current database format
Application	Warning	1	2020-09-08 11:54:26		ESENT	642: svchost (2908,D,35) SRUJet: The database format feature version 9120 (0x23a0) could not be used due to the current database format
Application	Warning	1	2020-09-08 11:54:26		ESENT	642: svchost (2908,D,40) SRUJet: The database format feature version 9080 (0x2378) could not be used due to the current database format
Application	Warning	1	2020-09-08 11:54:26		ESENT	642: svchost (2908,D,46) SRUJet: The database format feature version 9180 (0x23dc) could not be used due to the current database format
Application	Warning	1	2020-09-08 11:54:27		ESENT	642: Catalog Database (2868,D,40) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:27		ESENT	642: Catalog Database (2868,D,35) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-		ESENT	642: Catalog Database (2868,D,35) Catalog Database: The database format feature version 9120 (0x23a0) could not be used due to the curr

			08 11:54:27		Navigation
Application	Warning	1	2020-09-08 11:54:27	ESENT	642: Catalog Database (2868,D,40) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:27	ESENT	642: Catalog Database (2868,D,35) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:27	ESENT	642: Catalog Database (2868,D,35) Catalog Database: The database format feature version 9120 (0x23a0) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:34	ESENT	642: Catalog Database (2868,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:34	ESENT	642: Catalog Database (2868,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:34	ESENT	642: Catalog Database (2868,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:34	ESENT	642: Catalog Database (2868,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:45	ESENT	642: Catalog Database (2868,D,22) Catalog Database: The database format feature version 9120 (0x23a0) could not be used due to the curr
Application	Warning	1	2020-09-08 11:54:58	ESENT	642: services (616,D,50) ?The database format feature version 9180 (0x23dc) could not be used due to the current database format 1568.20
Application	Warning	1	2020-09-08 11:54:58	ESENT	642: services (616,D,12) ?The database format feature version 9080 (0x2378) could not be used due to the current database format 1568.20
Application	Warning	1	2020-09-08 11:54:58	ESENT	642: services (616,D,22) ?The database format feature version 9120 (0x23a0) could not be used due to the current database format 1568.20
Application	Warning	1	2020-09-08 11:56:52	ESENT	642: svchost (4316,D,35) ?The database format feature version 9180 (0x23dc) could not be used due to the current database format 1568.2
Application	Warning	1	2020-09-08 11:56:52	ESENT	642: svchost (4316,D,35) ?The database format feature version 9120 (0x23a0) could not be used due to the current database format 1568.2
Application	Warning	1	2020-09-08 11:56:52	ESENT	642: svchost (4316,D,60) ?The database format feature version 9080 (0x2378) could not be used due to the current database format 1568.2
Application	Warning	1	2020-09-08 11:58:12	ESENT	642: svchost (3340,D,50) SRUJet: The database format feature version 9180 (0x23dc) could not be used due to the current database format
Application	Warning	1	2020-09-08 11:58:15	Windows Search Service	1008: The Windows Search Service is starting up and attempting to remove the old search index {Reason: Full Index Reset}.
Application	Warning	1	2020-09-08 11:58:18	ESENT	642: SearchIndexer (1516,D,35) Windows: The database format feature version 9180 (0x23dc) could not be used due to the current databas
Application	Warning	1	2020-09-08 11:58:18	ESENT	642: SearchIndexer (1516,D,35) Windows: The database format feature version 9120 (0x23a0) could not be used due to the current databas
Application	Warning	1	2020-09-08 11:58:19	ESENT	642: wuaueng.dll (4392,D,35) SUS20ClientDataStore: The database format feature version 9180 (0x23dc) could not be used due to the curre
Application	Warning	1	2020-09-08 11:58:19	ESENT	642: wuaueng.dll (4392,D,35) SUS20ClientDataStore: The database format feature version 9120 (0x23a0) could not be used due to the curre
Application	Warning	None	2020-09-08	Software Protection Platform Service	1193: Failed to gather PKEY information for OEM:DM product key. Error: 0xC004E016 Product key: WJND6-YR6F8-629WF-9GQDC-TMQH2

			11:59:40			
Application	Warning	1	2020-09-08 11:59:40		ESENT	642: DllHost (5148,D,35) WebCacheLocal: The database format feature version 9180 (0x23dc) could not be used due to the current database
Application	Warning	1	2020-09-08 11:59:40		ESENT	642: DllHost (5148,D,35) WebCacheLocal: The database format feature version 9120 (0x23a0) could not be used due to the current database
Application	Warning	1	2020-09-08 11:59:42		ESENT	642: DllHost (6488,D,35) WebPlatStorage: The database format feature version 9180 (0x23dc) could not be used due to the current database
Application	Warning	1	2020-09-08 11:59:42		ESENT	642: DllHost (6488,D,35) WebPlatStorage: The database format feature version 9120 (0x23a0) could not be used due to the current database
Application	Warning	1	2020-09-08 11:59:43		ESENT	642: svchost (6768,D,50) ?The database format feature version 9180 (0x23dc) could not be used due to the current database format 1568.2
Application	Warning	1	2020-09-08 11:59:43		ESENT	642: qmgr.dll (6812,D,35) QmgrDatabaseInstance: The database format feature version 9180 (0x23dc) could not be used due to the current
Application	Warning	1	2020-09-08 11:59:43		ESENT	642: qmgr.dll (6812,D,35) QmgrDatabaseInstance: The database format feature version 9120 (0x23a0) could not be used due to the current
Application	Warning	None	2020-09-08 12:00:02		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Error	None	2020-09-08 12:00:14		SecurityCenter	16: Error while updating Windows Defender status to SECURITY_PRODUCT_STATE_ON.
Application	Error	101	2020-09-08 13:46:42		Application Hang	1002: The program acad.exe version 30.0.47.0 stopped interacting with Windows and was closed. To see if more information about the proble application ID: ? Hang type: Top level window is idle
Application	Error	100	2020-09-08 14:27:15		Application Error	1000: Faulting application name: DllHost.exe, version: 10.0.19041.1, time stamp: 0x415fabe9 Faulting module name: combase.dll, version: 643ecedbbb74 Faulting package full name: Microsoft.SkypeApp_15.64.78.0_x86__kzf8qxf38zg5c Faulting package-relative application ID: Ap
Application	Error	None	2020-09-08 14:52:47	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-08 14:52:47	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Warning	1	2020-09-08 14:53:40		ESENT	642: Catalog Database (2672,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-08 14:53:40		ESENT	642: Catalog Database (2672,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-08 14:54:05		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 14:54:14		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 14:55:42		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 17:15:22		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 17:15:32		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 17:15:49		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId

Application	Warning	None	2020-09-08 19:16:51	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reaso	f1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 19:17:09	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-08 20:46:16	ESENT	642: Catalog Database (3436,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-08 20:46:16	ESENT	642: Catalog Database (3436,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-08 20:46:42	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-08 20:46:54	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-09 01:23:07	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-09 01:25:22	ESENT	642: DllHost (2640,D,35) WebCacheLocal: The database format feature version 9180 (0x23dc) could not be used due to the current database
Application	Warning	1	2020-09-09 01:25:22	ESENT	642: DllHost (2640,D,35) WebCacheLocal: The database format feature version 9120 (0x23a0) could not be used due to the current database
Application	Warning	1	2020-09-09 01:25:29	ESENT	642: SettingSyncHost (1264,D,35) {4CB56D8C-D509-4DA8-9FBB-C30B76078AA5}: The database format feature version 9180 (0x23dc) coul
Application	Warning	1	2020-09-09 01:25:29	ESENT	642: SettingSyncHost (1264,D,35) {4CB56D8C-D509-4DA8-9FBB-C30B76078AA5}: The database format feature version 9120 (0x23a0) coul
Application	Warning	1	2020-09-09 01:25:31	ESENT	642: SettingSyncHost (1264,D,35) {2B2C3B1D-1CA3-427D-BD5A-A5B954C9824C}: The database format feature version 9180 (0x23dc) coul
Application	Warning	1	2020-09-09 01:25:31	ESENT	642: SettingSyncHost (1264,D,35) {2B2C3B1D-1CA3-427D-BD5A-A5B954C9824C}: The database format feature version 9120 (0x23a0) cou
Application	Warning	None	2020-09-09 01:26:49	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-09 01:27:05	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-09 01:27:28	ESENT	642: DllHost (3524,D,35) WebPlatStorage: The database format feature version 9180 (0x23dc) could not be used due to the current database
Application	Warning	1	2020-09-09 01:27:28	ESENT	642: DllHost (3524,D,35) WebPlatStorage: The database format feature version 9120 (0x23a0) could not be used due to the current database
Application	Warning	1	2020-09-09 01:27:28	ESENT	642: DllHost (3524,D,35) Microsoft.Windows.Search_cw5n1h2txyewy_NOEDP_LEGACY_IDB: The database format feature version 9180 (0x23
Application	Warning	1	2020-09-09 01:27:28	ESENT	642: DllHost (3524,D,35) Microsoft.Windows.Search_cw5n1h2txyewy_NOEDP_LEGACY_IDB: The database format feature version 9120 (0x23
Application	Warning	1	2020-09-09 01:32:28	ESENT	642: svchost (5552,D,35) Unistore: The database format feature version 9180 (0x23dc) could not be used due to the current database forma
Application	Warning	1	2020-09-09 01:32:28	ESENT	642: svchost (5552,D,35) Unistore: The database format feature version 9120 (0x23a0) could not be used due to the current database forma
Application	Warning	1	2020-09-	ESENT	642: DllHost (3524,D,35) WebPlatStorage: The database format feature version 9180 (0x23dc) could not be used due to the current database

			09 01:33:01			Navigation
Application	Warning	1	2020-09-09 01:33:01		ESENT	642: DllHost (3524,D,35) WebPlatStorage: The database format feature version 9120 (0x23a0) could not be used due to the current databas
Application	Warning	1	2020-09-09 01:33:03		ESENT	642: DllHost (3524,D,35) Internet_NOEDP_EDGE_IDB: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 01:33:03		ESENT	642: DllHost (3524,D,35) Internet_NOEDP_EDGE_IDB: The database format feature version 9120 (0x23a0) could not be used due to the curr
Application	Warning	1	2020-09-09 01:40:38		ESENT	642: Catalog Database (1228,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 01:40:38		ESENT	642: Catalog Database (1228,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 01:40:38		ESENT	642: Catalog Database (1228,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 01:40:38		ESENT	642: Catalog Database (1228,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 01:40:38		ESENT	642: Catalog Database (1228,D,22) Catalog Database: The database format feature version 9120 (0x23a0) could not be used due to the curr
Application	Warning	1	2020-09-09 01:42:45		ESENT	642: DllHost (11844,D,35) WebCacheLocal: The database format feature version 9180 (0x23dc) could not be used due to the current databas
Application	Warning	1	2020-09-09 01:42:45		ESENT	642: DllHost (11844,D,35) WebCacheLocal: The database format feature version 9120 (0x23a0) could not be used due to the current databas
Application	Error	None	2020-09-09 02:00:23		SideBySide	35: Activation context generation failed for "C:\Program Files (x86)\Microsoft Office\root\Office16\lync.exe.Manifest".Error in manifest or poli UccApi,processorArchitecture="x86",type="win32",version="16.0.0.0". Please use sxstrace.exe for detailed diagnosis.
Application	Error	None	2020-09-09 02:15:03	bebos	MsiInstaller	11500: Product: CSR Harmony Wireless Software Stack -- Error 1500.Another installation is in progress. You must complete that installation b
Application	Error	100	2020-09-09 02:15:17		Application Error	1000: Faulting application name: CsrBtService.exe, version: 2.1.63.0, time stamp: 0x4f6b2b7e Faulting module name: CsrBtService.exe, vers Harmony Wireless Software Stack\CsrBtService.exe Report Id: 431b0c91-2296-45e8-8152-97d35cbe4da1 Faulting package full name: ? Fault
Application	Warning	1	2020-09-09 02:18:47		ESENT	642: Catalog Database (2764,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 02:18:47		ESENT	642: Catalog Database (2764,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-09 02:19:17		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-09 02:19:27		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-09 17:51:19		ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 17:51:19		ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-09 17:51:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-09		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId

			17:52:09		
Application	Warning	None	2020-09-09 17:52:27	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Error	None	2020-09-09 17:57:22	Office 2016 Licensing Service	0: The operation completed successfully.
Application	Warning	None	2020-09-09 19:41:54	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-09 19:42:04	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-09 19:47:12	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:47:12	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:47:12	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:47:13	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:47:13	ESENT	642: Catalog Database (3612,D,22) Catalog Database: The database format feature version 9120 (0x23a0) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:31	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:31	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:31	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:31	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database Navigation 30 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:33	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:33	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:33	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:33	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			09 19:55:35		Navigation
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:35	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			19:55:36		
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:36	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:37	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:38	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:38	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:38	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:38	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database Navigation 30 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:39	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:40	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			09 19:55:41		Navigation
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:55:41	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:32	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:32	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:34	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:34	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:34	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:34	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:35	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:35	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:56:35	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:03	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:03	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:03	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:03	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			19:58:20		
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:20	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:21	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:21	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:21	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:21	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:39	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:39	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:39	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:58:39	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:49	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:49	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:49	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:49	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:49	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database Navigation 30 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:50	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			09 19:59:51		Navigation
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:51	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			19:59:52		
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:52	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database Navigation 80 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:53	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:54	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:55	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:55	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:55	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:55	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:55	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:55	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			09 19:59:56		

Navigation

Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:56	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:57	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:58	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			19:59:58		
Application	Warning	1	2020-09-09 19:59:58	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:58	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:58	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:58	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:58	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 19:59:59	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:00	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:00	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:00	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:00	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:03	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:03	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:03	ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:03	ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

Application	Warning	1	2020-09-09 20:00:04		ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database Navigation 30 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:04		ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:04		ESENT	642: Catalog Database (3612,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:04		ESENT	642: Catalog Database (3612,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:47		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:47		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:58		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:58		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:58		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:58		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:59		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:59		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:59		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:00:59		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-09 20:01:03	SYSTEM	Microsoft-Windows-WMI	63: A provider, DMWmiBridgeProv, has been registered in the Windows Management Instrumentation namespace root\cimv2\mdm\dmmap to
Application	Warning	None	2020-09-09 20:01:03	SYSTEM	Microsoft-Windows-WMI	63: A provider, DMWmiBridgeProv, has been registered in the Windows Management Instrumentation namespace root\cimv2\mdm\dmmap to
Application	Warning	None	2020-09-09 20:01:03	SYSTEM	Microsoft-Windows-WMI	63: A provider, DMWmiBridgeProv, has been registered in the Windows Management Instrumentation namespace root\cimv2\mdm\dmmap to
Application	Warning	None	2020-09-09 20:01:03	SYSTEM	Microsoft-Windows-WMI	63: A provider, DMWmiBridgeProv1, has been registered in the Windows Management Instrumentation namespace root\cimv2\mdm\dmmap t
Application	Warning	None	2020-09-09 20:01:03	SYSTEM	Microsoft-Windows-WMI	63: A provider, DMWmiBridgeProv1, has been registered in the Windows Management Instrumentation namespace root\cimv2\mdm\dmmap t
Application	Warning	None	2020-09-09 20:01:03	SYSTEM	Microsoft-Windows-WMI	63: A provider, DMWmiBridgeProv1, has been registered in the Windows Management Instrumentation namespace root\cimv2\mdm\dmmap t
Application	Warning	None	2020-09-09 20:01:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-		Software Protection	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId

			09 20:01:25	Platform Service	Navigation
Application	Warning	1	2020-09-09 20:01:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:01:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-09 20:01:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-09 20:01:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-10 15:57:22	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-10 15:57:32	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-10 15:57:48	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-10 16:00:07	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:07	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:07	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:07	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:00:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:52:55	ESENT	642: svchost (3460,D,35) DS_Token_DB: The database format feature version 9180 (0x23dc) could not be used due to the current database
Application	Warning	1	2020-09-10 16:52:55	ESENT	642: svchost (3460,D,35) DS_Token_DB: The database format feature version 9120 (0x23a0) could not be used due to the current database
Application	Warning	1	2020-09-10 16:52:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:52:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:52:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			16:52:58		
Application	Warning	1	2020-09-10 16:52:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:52:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:52:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:52:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:21	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:21	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:21	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:21	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:24	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:24	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:24	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:24	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:32	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:32	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:32	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:32	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:34	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:34	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:34	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:34	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 16:53:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database	30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:53:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:53:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:53:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:53:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:53:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:53:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:54:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	

			10 16:59:01		Navigation
Application	Warning	1	2020-09-10 16:59:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:03	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:04	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:04	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:04	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:23	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:23	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:23	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:23	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:32	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:32	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:32	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			16:59:32		
Application	Warning	1	2020-09-10 16:59:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 16:59:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database	0 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 16:59:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 16:59:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:07	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:07	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:07	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:07	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:21	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:22	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:22	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:22	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:25	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:25	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:25	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:25	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:26	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:26	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:26	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:26	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:00:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	

			10 17:00:38		

Navigation

Application	Warning	1	2020-09-10 17:00:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:28:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:14	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:14	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:14	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:14	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:16	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:16	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:16	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:29:16		
Application	Warning	1	2020-09-10 17:29:34	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:35	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:35	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:35	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:44	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:44	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:29:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 80 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:29:57		Navigation
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:29:58		
Application	Warning	1	2020-09-10 17:29:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:29:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:00	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:30:00	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:00	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:00	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:01	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:30:09		Navigation
Application	Warning	1	2020-09-10 17:30:09	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:19	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:19	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:19	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:19	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:25	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:25	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:25	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:25	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:26	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:26	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:26	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:26	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:30:45		
Application	Warning	1	2020-09-10 17:30:52	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:52	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:52	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:52	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:54	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:54	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:54	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:54	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:55	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:55	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:55	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:55	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:30:57	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 80 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:57	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:30:59		

Navigation

Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:30:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:04	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:04	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:04	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:31:04		
Application	Warning	1	2020-09-10 17:31:05	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:05	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:05	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:05	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:17	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:17	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:17	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:17	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:22	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:22	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:22	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:22	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:28	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:31:33		Navigation
Application	Warning	1	2020-09-10 17:31:33	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:37	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:31:38		
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:38	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:39	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:31:40		Navigation
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:40	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:31:41		
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:41	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:42	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:43	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:31:44		Navigation
Application	Warning	1	2020-09-10 17:31:44	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:45	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:31:45		
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:46	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:47	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			10 17:31:48		Navigation
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:48	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:31:49		
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:49	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:50	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database	30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:51	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:52	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:52	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:52	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:52	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	

			10 17:31:53		Navigation
Application	Warning	1	2020-09-10 17:31:53	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:54	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:56	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			17:31:58		
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:58	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:31:59	ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01	ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-10 17:32:01		ESENT	642: Catalog Database (2692,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Error	None	2020-09-10 17:40:49	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by servic
Application	Error	None	2020-09-10 17:40:49	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by servic
Application	Error	None	2020-09-10 18:19:46	bebos	Microsoft-Windows-User Profiles Service	1515: Windows has backed up this user profile. Windows will automatically try to use the backup profile the next time this user logs on.
Application	Error	None	2020-09-10 18:19:46	bebos	Microsoft-Windows-User Profiles Service	1511: Windows cannot find the local profile and is logging you on with a temporary profile. Changes you make to this profile will be lost when
Application	Error	None	2020-09-10 18:19:46	bebos	Microsoft-Windows-User Profiles Service	1500: Windows cannot log you on because your profile cannot be loaded. Check that you are connected to the network, and that your networ
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\SecurityHealthService.exe, PID: 8448, Pr
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 896, ProfSvc PID: 143
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 896, ProfSvc PID: 143
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2680, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\SecurityHealthService.exe, PID: 8448, Pr
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 6888, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2680, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2680, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\csrss.exe, PID: 5444, ProfSvc PID: 1432
Application	Error	None	2020-09-	SYSTEM	Microsoft-Windows-	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 1828, ProfSvc PID: 14

			10 18:19:46		User Profiles Service	Navigation
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 896, ProfSvc PID: 143
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1542: Windows cannot load classes registry file. DETAIL - Access is denied.
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-10 18:19:46	SYSTEM	Microsoft-Windows-User Profiles Service	1508: Windows was unable to load the registry. This problem is often caused by insufficient memory or insufficient security rights. DETAIL - A
Application	Warning	None	2020-09-10 18:19:46		Wlclntfy	6004: The winlogon notification subscriber <Profiles> failed a critical notification event.
Application	Warning	None	2020-09-10 18:19:50		Wlclntfy	6001: The winlogon notification subscriber <Sens> failed a notification event.
Application	Warning	None	2020-09-10 18:19:50		Wlclntfy	6001: The winlogon notification subscriber <Profiles> failed a notification event.
Application	Error	None	2020-09-10 18:19:56	bebos	Microsoft-Windows-User Profiles Service	1511: Windows cannot find the local profile and is logging you on with a temporary profile. Changes you make to this profile will be lost when
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\SecurityHealthService.exe, PID: 8448, Pr
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 896, ProfSvc PID: 143
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 896, ProfSvc PID: 143
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2680, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\SecurityHealthService.exe, PID: 8448, Pr
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 6888, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2680, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2680, ProfSvc PID: 14
Application	Error	None	2020-09-10 18:19:56	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 896, ProfSvc PID: 143
Application	Warning	1	2020-09-10 18:19:59		ESENT	642: taskhostw (10168,D,35) WebCacheLocal: The database format feature version 9180 (0x23dc) could not be used due to the current data
Application	Warning	1	2020-09-10		ESENT	642: taskhostw (10168,D,35) WebCacheLocal: The database format feature version 9120 (0x23a0) could not be used due to the current data

			18:19:59			
Application	Warning	None	2020-09-10 18:20:06		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-10 18:20:16		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-10 18:20:18		ESENT	642: DllHost (13196,D,35) Microsoft.Windows.Search_cw5n1h2txyewy_NOEDP_LEGACY_IDB: The database format feature version 9180 (0x2
Application	Warning	1	2020-09-10 18:20:18		ESENT	642: DllHost (13196,D,35) Microsoft.Windows.Search_cw5n1h2txyewy_NOEDP_LEGACY_IDB: The database format feature version 9120 (0x2
Application	Warning	1	2020-09-10 18:20:18		ESENT	642: DllHost (13196,D,35) WebPlatStorage: The database format feature version 9180 (0x23dc) could not be used due to the current databas
Application	Warning	1	2020-09-10 18:20:18		ESENT	642: DllHost (13196,D,35) WebPlatStorage: The database format feature version 9120 (0x23a0) could not be used due to the current databa
Application	Error	None	2020-09-10 18:20:20		SideBySide	35: Activation context generation failed for "C:\Program Files (x86)\Microsoft Office\root\Office16\lync.exe.Manifest".Error in manifest or polic UccApi,processorArchitecture="x86",type="win32",version="16.0.0.0". Please use sxstrace.exe for detailed diagnosis.
Application	Error	None	2020-09-10 18:20:27	SYSTEM	Microsoft-Windows-User Profiles Service	1533: Windows cannot delete the profile directory C:\Users\TEMP. This error may be caused by files in this directory being used by another pr
Application	Warning	None	2020-09-10 18:20:32		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-10 18:21:06		ESENT	642: Catalog Database (3492,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 18:21:06		ESENT	642: Catalog Database (3492,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-10 18:21:30		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-10 18:21:39		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-10 18:53:06		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-10 19:20:29		ESENT	642: Catalog Database (3020,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-10 19:20:29		ESENT	642: Catalog Database (3020,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-10 19:20:51		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-10 19:21:01		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 11:22:10		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 11:22:22		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 11:22:40		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId

Application	Warning	1	2020-09-11 11:39:40	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:39:40	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-11 11:40:00	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:57	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:58	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:58	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:58	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:58	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			11 11:53:59		Navigation
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:53:59	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:00	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:06	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:06	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:06	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:54:06		
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:07	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:15	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:15	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:15	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:15	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:16	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:16	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:16	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:16	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			11 11:54:17		Navigation
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:17	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:54:17		
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:18	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:19	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:19	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:19	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:19	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database	30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:20	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	

			11 11:54:21		Navigation
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:21	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:54:22		
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:22	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:23	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:23	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:23	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:23	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:24	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:25	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:54:25	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database	30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:25	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:25	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:26	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	

			11 11:54:27		Navigation
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:54:28		
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:28	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:29	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:29	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:29	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:29	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:41	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:43	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:46	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:46	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:46	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:46	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			11 11:54:47		Navigation
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:47	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:48	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:48	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:48	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:54:48	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:55:10		
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:10	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database	30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr	
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr	

			11 11:55:12		Navigation
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:12	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:55:13		
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:55:13	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:14	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:15	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:25	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:25	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:25	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:25	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:27	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:27	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:29	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:29	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:29	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:29	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:29	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:30	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

			11 11:59:30		

Navigation

Application	Warning	1	2020-09-11 11:59:30	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:30	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:30	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:30	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:30	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:42	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:42	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:42	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:42	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:52	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:53	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:53	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr

			11:59:53		
Application	Warning	1	2020-09-11 11:59:54	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:54	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:54	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:54	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:55	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:55	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:55	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:55	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56	ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr

Application	Warning	1	2020-09-11 11:59:56		ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56		ESENT	642: Catalog Database (2264,D,50) Catalog Database: The database format feature version 9180 (0x23dc) could not be used due to the curr
Application	Warning	1	2020-09-11 11:59:56		ESENT	642: Catalog Database (2264,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-11 12:17:42		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 14:17:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Error	None	2020-09-11 14:40:25	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-11 14:40:25	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\SecurityHealthService.exe, PID: 3668, Pr
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 924, ProfSvc PID: 130
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 924, ProfSvc PID: 130
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\SecurityHealthService.exe, PID: 3668, Pr
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 4956, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 1396, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2220, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 1396, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2220, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-	SYSTEM	Microsoft-Windows-	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 1396, ProfSvc PID: 13

			11 18:12:09		User Profiles Service	
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2220, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 1396, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2220, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\csrss.exe, PID: 588, ProfSvc PID: 1300.
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 924, ProfSvc PID: 130
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 1396, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2220, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 2380, ProfSvc PID: 13
Application	Error	None	2020-09-11 18:12:09	SYSTEM	Microsoft-Windows-User Profiles Service	1552: User hive is loaded by another process (Registry Lock) Process name: C:\Windows\System32\svchost.exe, PID: 5632, ProfSvc PID: 13
Application	Warning	None	2020-09-11 18:12:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 18:12:46		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 18:13:07		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-11 19:54:37		ESENT	642: Catalog Database (3020,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-11 19:54:37		ESENT	642: Catalog Database (3020,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-11 19:55:02		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-11 19:55:12		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 11:21:14		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 11:21:33		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId

			11:21:49			
					Navigation	
Application	Warning	1	2020-09-12 11:26:22		ESENT	642: Catalog Database (2908,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-12 11:26:23		ESENT	642: Catalog Database (2908,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-12 11:26:52		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 11:27:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 11:50:00		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 11:50:10		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	1	2020-09-12 11:51:38		ESENT	642: Catalog Database (3032,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-12 11:51:38		ESENT	642: Catalog Database (3032,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-12 11:52:07		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 11:52:17		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Error	101	2020-09-12 13:29:01		Application Hang	1002: The program explorer.exe version 10.0.19041.488 stopped interacting with Windows and was closed. To see if more information about type: Unknown
Application	Warning	None	2020-09-12 13:52:25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 15:52:25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Error	None	2020-09-12 16:14:54	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Error	None	2020-09-12 16:14:54	SYSTEM	Microsoft-Windows-User Profiles Service	1512: Windows cannot unload your registry file. The memory used by the registry has not been freed. This problem is often caused by service
Application	Warning	1	2020-09-12 16:15:31		ESENT	642: Catalog Database (3056,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-12 16:15:31		ESENT	642: Catalog Database (3056,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-12 16:16:00		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 16:16:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 18:46:33		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId
Application	Warning	None	2020-09-12 18:46:42		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId

Application	Warning	1	2020-09-12 19:07:38	ESENT	642: Catalog Database (3032,D,12) Catalog Database: The database Navigation 30 (0x2378) could not be used due to the curr
Application	Warning	1	2020-09-12 19:07:38	ESENT	642: Catalog Database (3032,D,12) Catalog Database: The database format feature version 9080 (0x2378) could not be used due to the curr
Application	Warning	None	2020-09-12 19:08:06	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Application	Warning	None	2020-09-12 19:08:18	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Application	Warning	None	2020-09-12 20:22:47	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Application	Warning	None	2020-09-12 20:48:14	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Application	Warning	None	2020-09-12 20:48:37	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Application	Warning	None	2020-09-12 20:48:48	Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x800705B4 AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuIc
Security	Audit Success	12288	2020-09-08 01:43:46	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Acc which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to
Security	Audit Success	12288	2020-09-08 01:43:46	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Acc which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to
Security	Audit Success	12544	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:44:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 01:46:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 01:46:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12288	2020-09-08 01:46:35	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Acco which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to
Security	Audit Success	12288	2020-09-08 01:46:35	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Acco which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to
Security	Audit Success	13824	2020-09-08 01:47:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:47:23		
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 01:47:23	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 01:47:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13312	2020-09-08 11:54:05	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:05	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-08 11:54:05	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-08 11:54:05	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-08 11:54:06	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc

			11:54:09		used when User Account Control is enabled and the user chooses to st Navigation n as administrator. An elevated token is also u application does not require administrative privilege, and the user doe rogram using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:54:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon 0x220 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generated when a pro
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon 0x290 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x290 Process Name: C:\Windows\System32\winlogo was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation l participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates th
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x220 Process Name: C:\Windows\System32\wininit.e was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation l participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates th
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-0 Account Name: UMFD-0 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	13568	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xe8ef
Security	Audit	13569	2020-09-	Microsoft-Windows-	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log

	Success		08 11:54:10	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4720: A user account was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 New Acc Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 Allowed To Delegate To: - Old UAC V
Security	Audit Success	13824	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: 0x15 New UAC Value: 0x11 User Account Control: %%2050 User Parameters: - S
Security	Audit Success	13824	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID History: - Lo
Security	Audit Success	13824	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID History: - Lo
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:

			11:54:10		

Navigation

Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4731: A security-enabled local group was created. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID:
Security	Audit Success	13826	2020-09-08 11:54:10	Microsoft-Windows-Security-Auditing	4728: A member was added to a security-enabled global group. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain:
Security	Audit Success	12544	2020-09-08 11:54:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:54:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon 0x290 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a
Security	Audit Success	12544	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x290 Process Name: C:\Windows\System32\w computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x290 Process Name: C:\Windows\System32\w computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage

Security	Audit Success	12548	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12544	2020-09-08 11:54:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:54:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08	Microsoft-Windows-Security-Auditing	4718: System security access was removed from an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ?

			11:54:22		

Navigation

Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4717: System security access was granted to an account. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Log
Security	Audit Success	13569	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4739: Domain Policy was changed. Change Type: <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Pro <EventRecordID>94</EventRecordID><Correlation ActivityID='{130ce4a1-859c-0002-d4e5-0c139c85d601}'/><Execution ProcessID='680' <EventPayload>500061007300730077006F00720064002000500006F006C00690063007900000004D0049004E00570049004E00500043000000 </ProcessingErrorData></Event> modified Subject: Security ID: (null) Account Name: (null) Account Domain: (null) Logon ID: (null) Domain Domain Mode: (null) Domain Behavior Version: (null) OEM Information: (null) Additional Information: Privileges: (null)
Security	Audit Success	13824	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4725: A user account was disabled. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A
Security	Audit Success	13824	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A Group ID: - AllowedToDelegateTo: - Old UAC Value: 0x210 New UAC Value: 0x211 User Account Control: %%2080 User Parameters: - SID Hi
Security	Audit Success	13824	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4725: A user account was disabled. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A
Security	Audit Success	13824	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A ID: - AllowedToDelegateTo: - Old UAC Value: 0x214 New UAC Value: 0x215 User Account Control: %%2080 User Parameters: - SID History:
Security	Audit Success	13826	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Dom
Security	Audit Success	13826	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain:
Security	Audit Success	13826	2020-09-08 11:54:22	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain:
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N

			11:54:23		accessed. The subject fields indicate the account on the local system w . This is most commonly a service such as the a remote logon request originated. Workstation name is not always av ank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0
Security	Audit Success	13824	2020-09-08 11:54:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0
Security	Audit Success	101	2020-09-08 11:54:24	Microsoft-Windows-Eventlog	1108: The event logging service encountered an error while processing an incoming event published from Microsoft-Windows-Security-Auditin
Security	Audit Success	12544	2020-09-08 11:54:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:54:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0
Security	Audit Success	13824	2020-09-08 11:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0
Security	Audit Success	12292	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e

	Success		08 11:54:25	Security-Auditing	{00000000-0000-0000-0000-000000000000} Process Information: P Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system Navigation . This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			11:54:25		
Security	Audit Success	12292	2020-09-08 11:54:26	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-08 11:55:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:55:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:55:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:55:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:55:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:55:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:55:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:55:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:56:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:56:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:56:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:56:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:56:51	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e7 Target A Group ID: - AllowedToDelegateTo: - Old UAC Value: 0x211 New UAC Value: 0x211 User Account Control: - User Parameters: - SID History: -
Security	Audit Success	12544	2020-09-08 11:56:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:56:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N

			11:56:53		accessed. The subject fields indicate the account on the local system w . This is most commonly a service such as the a remote logon request originated. Workstation name is not always av ank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:56:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12544	2020-09-08 11:56:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:56:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:56:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:56:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:56:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:56:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:57:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:57:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:57:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: MINWINPC$ Account Domain: ? Logon ID: 0x3e {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x268 Process Name: C:\Windows\System32\services.exe N accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level fie in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of t
Security	Audit Success	12548	2020-09-08 11:57:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	103	2020-09-08 11:57:28	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-08 11:57:44	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:44	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-08 11:57:44	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:44	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0?????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit	13573	2020-09-	Microsoft-Windows-	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings

	Success		08 11:57:44	Security-Auditing	Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-08 11:57:45	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:52	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x24c Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This even
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x24c Process Name: C:\Wi on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most comm network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x2b0 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This ev
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x2b0 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This ev
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n

					on. The network fields indicate where a remote logon request originat ot always available and may be left blank in s intermediate services have participated in this logon request. - Packag ub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	13312	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-08 11:57:53	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xaefc
Security	Audit Success	12544	2020-09-08 11:57:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:57:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:57:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is r on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-08 11:57:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12548	2020-09-08 11:57:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:57:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12544	2020-09-08 11:58:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:58:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:58:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:58:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng

Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12290	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12290	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation: '
Security	Audit Success	12292	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation: '
Security	Audit Success	12292	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID 0x0
Security	Audit Success	12292	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI

	Success		08 11:58:10	Security-Auditing	Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account o Navigation equested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			11:58:10		

Navigation

Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	13826	2020-09-08 11:58:10	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	12292	2020-09-08 11:58:11	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-08 11:58:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:58:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13568	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORK S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13824	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4720: A user account was created. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon %%1793 User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 Allowed To Delegate T
Security	Audit Success	13824	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4722: A user account was enabled. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo
Security	Audit Success	13824	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo Path: %%1793 User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedToDeleg
Security	Audit Success	13826	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4728: A member was added to a security-enabled global group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account
Security	Audit Success	13826	2020-09-08 11:58:12	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account D
Security	Audit Success	13824	2020-09-08 11:58:13	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo Path: %%1793 User Workstations: %%1793 Password Last Set: 9/7/2020 9:58:13 PM Account Expires: %%1794 Primary Group ID: 513 All
Security	Audit Success	13824	2020-09-08 11:58:13	Microsoft-Windows-Security-Auditing	4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Do
Security	Audit Success	13824	2020-09-08 11:58:13	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo Path: %%1793 User Workstations: %%1793 Password Last Set: 9/7/2020 9:58:13 PM Account Expires: %%1794 Primary Group ID: 513 All
Security	Audit Success	13824	2020-09-08 11:58:13	Microsoft-Windows-Security-Auditing	4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Do
Security	Audit Success	13826	2020-09-08	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc

			11:58:14		
Security	Audit Success	13826	2020-09-08 11:58:14	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-08 11:58:14	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account D
Security	Audit Success	12544	2020-09-08 11:58:15	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x604 Process Name: C:\Windows\System32\oobe\msoobe.exe Network Information: Network Address: - Port: - Th
Security	Audit Success	12544	2020-09-08 11:58:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Logon ID: 0x43a80 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 11:58:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Logon ID: 0x43a39 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-08 11:58:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13826	2020-09-08 11:58:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-08 11:58:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-08 11:58:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-08 11:58:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-08 11:58:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:58:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 11:58:19	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-08 11:58:19	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-08 11:58:19	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12290	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12290	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	12292	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:

Security	Audit Success	12292	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-18 Accou VQ$ Account Domain: WORKGROUP Logon ID 0x0
Security	Audit Success	13824	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12290	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	12290	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHO

	Success		08 11:58:26	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-08 11:58:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	12544	2020-09-08 11:59:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:59:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0xad8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Logon ID: 0x6c07f Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request
Security	Audit Success	12544	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI ID: 0x6c057 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			11:59:33		

Navigation

Security	Audit Success	12548	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: d
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-08 11:59:33	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Failure	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Failure	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Failure	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Failure	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Success	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Success	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

Security	Audit Success	12290	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Accou Navigation Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account D Key File Operation Information: File Path: C:\Users\defaultuser0\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account D Key File Operation Information: File Path: C:\Users\defaultuser0\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc %%2500 Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc %%2500 Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc %%2500 Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13826	2020-09-08 11:59:34	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	12290	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	12544	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S

			11:59:35		computer that was accessed. The subject fields indicate the account o equested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation r le and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-08 11:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	12544	2020-09-08 11:59:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:59:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:59:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] Navigation : WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S

			11:59:43		computer that was accessed. The subject fields indicate the account o equested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation r le and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-08 11:59:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

Security	Audit Success	13826	2020-09-08 11:59:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S -18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	13826	2020-09-08 11:59:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	12544	2020-09-08 12:00:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 12:00:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 12:00:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 12:00:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 12:00:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 12:00:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 12:00:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 12:00:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 12:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-08 12:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x780 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This ev
Security	Audit Success	12544	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x780 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x780 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This ev
Security	Audit Success	12544	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x780 Process Nan is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This i on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x780 Process Nan is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This i

					on. The network fields indicate where a remote logon request originat Navigation ot always available and may be left blank in s intermediate services have participated in this logon request. - Packag ub-protocol was used among the NTLM protoc
Security	Audit Success	12545	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account
Security	Audit Success	12548	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	13824	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12545	2020-09-08 12:02:00	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12545	2020-09-08 12:02:26	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-08 12:02:26	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12290	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Success	12292	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account D Key File Operation Information: File Path: C:\Users\defaultuser0\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1
Security	Audit Success	12292	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc %%2500 Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0xad8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Logon ID: 0xe885f Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request
Security	Audit Success	12544	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI ID: 0xe8837 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: d
Security	Audit Success	13826	2020-09-08 12:02:28	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit	12544	2020-09-	Microsoft-Windows-	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain

	Success		08 12:03:32	Security-Auditing	Information: Process ID: 0x4b0 Process Name: C:\Windows\System3 Navigation nformation: Network Address: - Port: - This ev
Security	Audit Success	12544	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4b0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x4b0 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This ev
Security	Audit Success	12544	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4b0 Process Nan is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4b0 Process Nan is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12545	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account
Security	Audit Success	12545	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-2 Account Name: UMFD-2 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manage
Security	Audit Success	13824	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-08 12:03:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12288	2020-09-08 13:46:36	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Acc which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to
Security	Audit Success	12288	2020-09-08 13:46:36	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Acc which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to
Security	Audit Success	13824	2020-09-08 13:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			13:46:43		

Navigation

Security	Audit Success	13824	2020-09-08 13:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-08 13:47:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 13:47:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 13:47:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 13:47:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 13:48:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:48:32		
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 13:48:32	Security-Auditing	
Security	Audit Success	13824	2020-09-08 13:48:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:48:34		

Navigation

Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:48:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		08 13:49:10	Security-Auditing	
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:49:10		
					Navigation
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:49:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 13:54:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 13:54:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 13:55:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 13:55:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:55:27		
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:55:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 13:55:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 13:55:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 13:55:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 13:55:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-08 13:55:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 13:55:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:00:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:00:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:00:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:00:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:00:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:00:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:02:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-08 14:03:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Failure		08 14:03:01	Security-Auditing	Navigation
Security	Audit Failure	12290	2020-09-08 14:03:02	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-08 14:03:02	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:03:02	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-08 14:03:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:03:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:03:08	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Contro
Security	Audit Success	12544	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:03:09	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:10		
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:03:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:03:41	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:42		
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:03:44	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:44		
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:03:44	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:44		

Navigation

Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:03:45	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:45		
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:03:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:04:04	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:04:04		Navigation
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:04:04	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:04:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [redacted] Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:20:34	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:20:34		

Navigation

Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:20:35	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:20:35		
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:20:36	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:20:36		
Security	Audit Success	13824	2020-09-08 14:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:20:40	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:20:43		
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:20:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:25:28		
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-08 14:25:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	12544	2020-09-08 14:27:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:27:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:29:52		

Navigation

Security	Audit Success	13824	2020-09-08 14:29:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:29:53	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:29:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:31:52		

Navigation

Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Contro

Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:31:53	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:31:53		
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:31:54	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:31:54		
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:31:55	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:31:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:31:59		
Security	Audit Success	13824	2020-09-08 14:31:59	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:31:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\04385e8bbe7aff4951c0ac8fa1dceb92_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	13824	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:32:02	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			14:32:02		
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

	Success		08 14:32:02	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:32:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:03		
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:32:03	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:03		
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:32:03	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:03		

Navigation

Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:32:04	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:04		
					Navigation
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:32:18	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:18		
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12290	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:32:19	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:19		
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:32:19	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:19		
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:32:19	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:20		
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:32:20	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			14:32:21		
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:32:21	Security-Auditing	

Navigation

Security	Audit Success	12290	2020-09-08 14:32:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-08 14:32:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:32:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:32:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:32:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:32:40	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:40		
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:32:41	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:41		
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:32:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:32:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:32:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:32:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:32:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:35:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12290	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0	
Security	Audit Success	12290	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7	
Security	Audit Success	12292	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 P C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4ecf03c26e8df7f8523c1a8f928b030b_970e8aca-7c00-49	
Security	Audit Success	12292	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7 Proce C:\ProgramData\Microsoft\Crypto\SystemKeys\b1e0768a3091627204a208d86f9cc86d_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:	
Security	Audit Success	12292	2020-09-08 14:35:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7	
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		08 14:36:21	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:36:21		

Navigation

Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:36:22	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:36:22		
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:36:22	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:36:22		
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:42:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:42:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:42:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			14:49:08		

Navigation

Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:49:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:49:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:49:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:49:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12548	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se[illegible] Navigation [illegible]t Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:52:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	103	2020-09-08 14:53:20	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-08 14:53:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:32	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-08 14:53:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-08 14:53:32	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-08 14:53:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2b4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b4 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit	12544	2020-09-	Microsoft-Windows-	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK

	Success		08 14:53:36	Security-Auditing	Process ID: 0x250 Process Name: C:\Windows\System32\wininit.exe Navigation work Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x250 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is r on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc

			14:53:36		used when User Account Control is enabled and the user chooses to st n as administrator. An elevated token is also u application does not require administrative privilege, and the user doe rogram using Run as administrator.
Security	Audit Success	13312	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-08 14:53:36	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xafbc
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2b4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		08 14:53:37	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s

			14:53:39		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 14:53:39	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-08 14:53:40	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5cc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3a34b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x39f3b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces

			14:53:41		Length: 0 This event is generated when a logon session is created. It ıter that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logge dicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13826	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 14:53:41	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 14:53:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-08 14:53:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:53:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:53:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:53:47	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:53:47		
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:53:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:53:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 14:53:53	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 14:53:53	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:53:54		
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			14:53:55		
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:53:55	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:53:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:54:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:54:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 14:54:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:54:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:54:05	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12290	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5cc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xdb0e1 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi

					for whom the new logon was created, i.e. the account that was logged correlate this event with a KDC event. - Transited services indicate wh
Security	Audit Success	12544	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xdb09c Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2ec Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0xdc5c9 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12544	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0xdc54a Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12545	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 14:54:06	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:09		Navigation
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:54:09	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:09		

Navigation

Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:54:10	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:10		Navigation
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:54:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:54:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:54:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:12		

Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-08 14:54:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 14:54:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		08 14:54:19	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:19		

Navigation

Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:54:19	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:20		
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:54:20	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:20		
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:54:20	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:54:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49I
Security	Audit Success	12292	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:32		
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:54:32	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:54:33	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:54:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:34	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:54:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:54:35		
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:54:35	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:54:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 14:54:41	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:54:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:54:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12290	2020-09-08 14:55:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:55:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			14:55:07		
Security	Audit Success	13824	2020-09-08 14:55:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:55:11	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:55:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			14:55:12		
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:55:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:55:13	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-08 14:55:18	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12544	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x13e8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x13e8 Process Name: C:\Windows\ the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x13e8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x13e8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x13e8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12545	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	13824	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			14:55:19		

Navigation

Security	Audit Success	13824	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 14:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12545	2020-09-08 14:55:20	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-08 14:55:20	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12292	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5cc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x1f8ed6 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x1f8e91 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 14:55:24	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12290	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2ec Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x1f93b9 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind

Security	Audit Success	12544	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] \ETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x1f9355 Network Account Name: - Network Account Dom Navigation)000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-08 14:55:25	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-08 14:55:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:40	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-08 14:55:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:55:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:55:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		08 14:55:41	Security-Auditing	
Security	Audit Success	12544	2020-09-08 14:55:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:55:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 14:55:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 14:55:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:55:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 14:55:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 14:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:55:48		
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:55:48	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12544	2020-09-08 14:56:26	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account (x86)\Microsoft\Edge\Application\msedge.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type f be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited se
Security	Audit Success	13824	2020-09-08 14:56:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 14:56:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		08 14:56:32	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 14:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:56:34		
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 14:56:35	Security-Auditing	
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:56:36		
Security	Audit Success	13824	2020-09-08 14:56:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 14:56:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 14:56:37	Security-Auditing	

Navigation

Security	Audit Success	12544	2020-09-08 15:00:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:00:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 15:03:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:03:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 15:03:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 15:03:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:03:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 15:03:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 15:04:05	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:04:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 15:08:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 15:08:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:08:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 15:08:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 15:10:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 15:10:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:10:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 15:10:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 15:10:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 15:10:27	Security-Auditing	
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:10:27		
					Navigation
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 15:10:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 15:11:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0xdc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generate

Security	Audit Success	12544	2020-09-08 15:11:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation IETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 ocess ID: 0xdc Process Name: C:\Windows\Sy computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0xdc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0xdc Process Name: C:\Win generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0xdc Process Name: C:\Win generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 15:12:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12545	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-2 Account Name: UMFD-2 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 15:12:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12545	2020-09-08 15:12:02	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0

Security	Audit Success	12545	2020-09-08 15:12:02	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-2 Navigation :count Domain: Window Manager Logon ID: 0
Security	Audit Success	12544	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5cc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x351c57 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x351c00 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-08 17:14:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-08 17:14:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-08 17:14:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-08 17:14:58	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-08 17:14:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 17:14:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 17:14:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	12544	2020-09-08 17:15:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 17:15:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:15:03		

Navigation

Security	Audit Success	13824	2020-09-08 17:15:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 17:15:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 17:15:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 17:15:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12292	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5cc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3ae97c Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3ae924 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2ec Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3b0975 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3b08f9 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-08	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

			17:15:09		

Navigation

Security	Audit Success	12545	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13826	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 17:15:09	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-08 17:15:14	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 17:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 17:15:26	Security-Auditing	
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:15:26		
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12544	2020-09-08 17:16:05	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account (x86)\Microsoft\Edge\Application\msedge.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type f be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited se
Security	Audit Success	13824	2020-09-08 17:16:05	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 17:16:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			17:16:46		

Navigation

Security	Audit Success	13824	2020-09-08 17:16:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 17:16:49	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:16:51		
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		08 17:16:53	Security-Auditing	
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:16:53		

Navigation

Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:30:01		
					Navigation
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 17:30:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 18:13:22	Security-Auditing	
Security	Audit Success	12544	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 18:13:24	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 18:13:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 18:26:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 18:26:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 18:27:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 18:27:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 18:31:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 18:31:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12544	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [redacted] ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [redacted] x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 18:49:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-08 19:16:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:16:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-08 19:17:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 19:17:03	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5cc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x5c2ec5 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x5c2e80 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2ec Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event

Security	Audit Success	12544	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [redacted] ETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x5c667c Network Account Name: - Network Account Dom [redacted] 0000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x5c65c5 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 19:17:09	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-08 19:18:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:18:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 19:18:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:18:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 19:34:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 19:34:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:34:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			19:34:41		
Security	Audit Success	12544	2020-09-08 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 19:47:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 19:47:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:47:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 19:47:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 19:54:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 19:54:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:08:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:08:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:08:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:08:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:19:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:19:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:25:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:25:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13824	2020-09-08 20:29:11	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Acc Navigation Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-08 20:29:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:29:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:29:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:29:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:32:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:32:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:33:50		

Navigation

Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:33:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 20:35:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:35:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:35:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:35:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:35:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:35:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 20:35:53	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			20:35:53		
					Navigation
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		08 20:35:55	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:35:55		
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 20:35:55	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:35:55		

Navigation

Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 20:35:56	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:35:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:36:16		
Security	Audit Success	13824	2020-09-08 20:36:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:36:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		08 20:36:18	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 20:36:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:36:19		
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 20:36:21	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:36:21		

Navigation

Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:36:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:36:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:36:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:36:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:36:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:36:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:36:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12545	2020-09-08 20:45:36	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-08 20:45:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-08 20:45:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation ıt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 20:45:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 20:45:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 20:45:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	103	2020-09-08 20:45:52	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-08 20:46:08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:08	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-08 20:46:08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-08 20:46:08	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-08 20:46:09	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:11	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x240 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc

Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in se intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in se intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in se intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	13312	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce

			20:46:12		used when User Account Control is enabled and the user chooses to st Navigation n as administrator. An elevated token is also u application does not require administrative privilege, and the user doe rogram using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-08 20:46:12	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb0d7
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19518 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x191af Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		08 20:46:13	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 20:46:13	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 20:46:14	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit	13826	2020-09-	Microsoft-Windows-	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do

	Success		08 20:46:15	Security-Auditing	

Navigation

Security	Audit Success	13826	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 20:46:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-08 20:46:16	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-08 20:46:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 20:46:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 20:46:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:46:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:46:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	12544	2020-09-08 20:46:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] IETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:46:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 20:46:23	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 20:46:23	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 20:46:25	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:46:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12292	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x92e0e Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x92da3 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x9422d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

Security	Audit Success	12544	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] ETHOANG$ Account Domain: WORKGROUP Lo ID: 0x94193 Network Account Name: - Network Account Domain: - Lo [illegible] 00-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12545	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-08 20:46:27	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-08 20:46:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:46:34	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-08 20:46:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:46:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:46:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 20:46:40	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:46:42		

Navigation

Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:46:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:46:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 20:47:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:47:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4

			20:47:06		

Navigation

Security	Audit Success	12292	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	13824	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-08 20:47:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-08 20:47:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-08 20:47:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-08 20:47:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:47:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:47:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12544	2020-09-08 20:47:22	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account (x86)\Microsoft\Edge\Application\msedge.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type f be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited se
Security	Audit Success	13824	2020-09-08 20:47:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		08 20:47:26	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:47:26		
Security	Audit Success	13824	2020-09-08 20:47:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		08 20:47:28	Security-Auditing	
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:47:29		
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-08 20:47:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12544	2020-09-08 20:47:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-08 20:47:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	13826	2020-09-08 20:47:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-08 20:47:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	12544	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-08 20:48:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12544	2020-09-08 20:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	

			20:48:22		
Security	Audit Success	12544	2020-09-08 20:50:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:50:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-08 20:50:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-08 20:50:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-08 20:53:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:53:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-08 20:55:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:55:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:56:34	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			20:56:35		
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 20:56:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			21:01:14		

Navigation

Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 21:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-08 21:01:34	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x1788 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1788 Process Name: C:\Windows\ the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x1788 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1788 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1788 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-08 21:02:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12545	2020-09-08 21:02:54	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-08 21:02:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 21:02:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 21:02:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 21:02:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-08 21:02:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-08 21:02:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L

	Success		08 21:02:55	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-08 21:02:55	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-08 21:02:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-08 21:02:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12545	2020-09-08 21:02:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-08 21:02:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-09 01:20:47	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-09 01:20:47	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12290	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc
Security	Audit Success	12292	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account D Key File Operation Information: File Path: C:\Users\defaultuser0\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1
Security	Audit Success	12292	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Acc %%2500 Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0xad8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Logon ID: 0x118096 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request
Security	Audit Success	12544	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Logon ID: 0x11806e Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request
Security	Audit Success	12548	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13826	2020-09-09 01:20:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	12544	2020-09-09 01:20:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:20:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 01:20:51	Security-Auditing	
Security	Audit Success	12548	2020-09-09 01:20:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:21:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ii services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:21:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 01:21:21	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:21:21	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ii services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit	13824	2020-09-	Microsoft-Windows-	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR

Navigation

	Success		09 01:21:46	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc Path: %%1793 User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedToDeleg
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc Path: %%1793 User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedToDeleg
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UA(
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedToDelegateTo: - Old UA(
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc Profile Path: %%1793 User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedT
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc Profile Path: %%1793 User Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 AllowedT
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc %%1793 Profile Path: %%1793 User Workstations: %%1793 Password Last Set: 9/7/2020 9:54:10 PM Account Expires: %%1794 Primary G
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc %%1793 Profile Path: %%1793 User Workstations: %%1793 Password Last Set: 9/7/2020 9:54:10 PM Account Expires: %%1794 Primary G
Security	Audit Success	13824	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4781: The name of an account was changed: Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGR
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC

			01:21:46		
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC

Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4735: A security-enabled local group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WC
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4737: A security-enabled global group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: W
Security	Audit Success	13826	2020-09-09 01:21:46	Microsoft-Windows-Security-Auditing	4737: A security-enabled global group was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: W
Security	Audit Success	12544	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:22:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	12544	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name:
Security	Audit Success	12544	2020-09-09 01:23:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng

Security	Audit Success	12548	2020-09-09 01:23:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [redacted] SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:23:45	Microsoft-Windows-Security-Auditing	4720: A user account was created. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor Workstations: %%1793 Password Last Set: %%1794 Account Expires: %%1794 Primary Group ID: 513 Allowed To Delegate To: - Old UAC V
Security	Audit Success	13826	2020-09-09 01:23:45	Microsoft-Windows-Security-Auditing	4728: A member was added to a security-enabled global group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account
Security	Audit Success	13826	2020-09-09 01:23:45	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account D
Security	Audit Success	13826	2020-09-09 01:23:45	Microsoft-Windows-Security-Auditing	4732: A member was added to a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account D
Security	Audit Success	12544	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Process Information: Process ID: 0x2f0 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - Thi
Security	Audit Success	12544	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Linked Logon ID: 0x17a3e0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000000000(Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Linked Logon ID: 0x17a378 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000000000(Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Do
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4722: A user account was enabled. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: 0x15 New UAC Value: 0x210 User Account Control: %%2048
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters:
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

Navigation

	Success		09 01:23:46	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

			01:23:46		
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters:
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logc Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters:
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Do
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:23:46	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	12290	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation: '
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:23:49		
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: localhost Additional Information: localhost Process Information: Process ID: 0xfd0 Process Name: C:\Windows\System32\CloudExperi
Security	Audit Success	12544	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: de Domain: MicrosoftAccount Logon ID: 0x183320 Linked Logon ID: 0x183348 Network Account Name: - Network Account Domain: - Logon GUI Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was log logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate whic
Security	Audit Success	12544	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: de Domain: MicrosoftAccount Logon ID: 0x183348 Linked Logon ID: 0x183320 Network Account Name: - Network Account Domain: - Logon GUI Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was log logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate whic
Security	Audit Success	12545	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [redacted] Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Path: - User Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC
Security	Audit Success	13826	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	13826	2020-09-09 01:23:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	12544	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:23:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12544	2020-09-09 01:23:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:23:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:23:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:23:55		

Navigation

Security	Audit Success	13824	2020-09-09 01:23:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:23:56	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:23:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:24:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:24:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:24:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12290	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\a39d12b8804ca9f91fc9af30bb875d2f_970e8aca-7c00-4
Security	Audit Success	13824	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12290	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4ecf03c26e8df7f8523c1a8f928b030b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0

Security	Audit Success	12292	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Accou Navigation Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	13824	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:24:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12292	2020-09-09 01:24:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	13824	2020-09-09 01:24:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 01:24:14	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-09 01:24:14	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:14	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:14	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\b1e0768a3091627204a208d86f9cc86d_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	12292	2020-09-09 01:24:14	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID 0x0
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:24:15	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			01:24:15		

Navigation

Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12292	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account localhost Additional Information: localhost Process Information: Process ID: 0x12ac Process Name: C:\Windows\System32\oobe\UserOOBEBr
Security	Audit Success	12544	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: be MicrosoftAccount Logon ID: 0x1a086e Linked Logon ID: 0x1a08a7 Network Account Name: - Network Account Domain: - Logon GUID: {0000 Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on

					3 (network). The New Logon fields indicate the account for whom the Navigation e. the account that was logged on. The networ Logon GUID is a unique identifier that can be used to correlate this ev ansited services indicate which intermediate s
Security	Audit Success	12544	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: be MicrosoftAccount Logon ID: 0x1a08a7 Linked Logon ID: 0x1a086e Network Account Name: - Network Account Domain: - Logon GUID: {0000 Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The networ Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate s
Security	Audit Success	12545	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:16	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou User Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: -
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:24:30	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:24:40		
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:24:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:24:53	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:24:54		
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:24:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:24:58	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:24:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

			01:25:19		
Security	Audit Success	12545	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 Account
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4725: A user account was disabled. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo Path: %%1793 User Workstations: %%1793 Password Last Set: 9/7/2020 9:58:13 PM Account Expires: %%1794 Primary Group ID: 513 All
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13826	2020-09-09 01:25:19	Microsoft-Windows-Security-Auditing	4733: A member was removed from a security-enabled local group. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x14ec Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This e
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x14ec Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Information: Process ID: 0x14ec Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This e
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x14ec Process Na is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This i on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x14ec Process Na is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This i on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Process Information: Process ID: 0xad8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Linked Logon ID: 0x1b40f0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subje

					the account for whom the new logon was created, i.e. the account tha ork fields indicate where a remote logon requ used to correlate this event with a KDC event. - Transited services ind ervices have participated in this logon request
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Linked Logon ID: 0x1b40a2 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subje the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon requ used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain Process Information: Process ID: 0x2f0 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - Thi
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Linked Logon ID: 0x1b4463 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Linked Logon ID: 0x1b4437 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The i services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12545	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-3 Account Name: UMFD-3 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12545	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-4 Account Name: DWM-4 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-4 Account Name: DWM-4 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters
Security	Audit	13824	2020-09-	Microsoft-Windows-	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logo

	Success		09 01:25:20	Security-Auditing	- Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old [illegible] ue: - User Account Control: - User Parameters
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13826	2020-09-09 01:25:20	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Failure	12290	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: File Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8
Security	Audit Success	12292	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12545	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manager Logon ID: 0

Security	Audit Success	12548	2020-09-09 01:25:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:25:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Navigation

	Success		09 01:25:24	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:25		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:25:26	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:26		
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:26	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:26		
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:25:27	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:27		
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:27	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:27		
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:28	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:28		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:28	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:28		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:28	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:28		
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:28	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:28		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:25:29	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:29		
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:29	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:29		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:29	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:29		
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:29	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:29		
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:25:30	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:30		
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:25:31	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			01:25:31		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:25:32	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:32		
Security	Audit Success	13824	2020-09-09 01:25:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:25:38	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:25:38		

Navigation

Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:25:39	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:25:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:25:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:25:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:25:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Failure	12290	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

	Failure		09 01:26:06	Security-Auditing	Navigation
Security	Audit Success	12290	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:26:07		
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:26:07	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:40	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:26:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:26:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:26:49		
Security	Audit Success	13824	2020-09-09 01:26:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:26:50	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:27:03	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:27:04		

Navigation

Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12544	2020-09-09 01:27:06	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account (x86)\Microsoft\Edge\Application\msedge.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type f be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited se
Security	Audit Success	13824	2020-09-09 01:27:06	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: Navigation
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:27:24	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:27:24		
					Navigation
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:27:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:27:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-09 01:27:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:27:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:27:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:27:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:27:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:27:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:27:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:27:37	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:27:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:27:39		
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:27:39	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:27:39		
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:27:40	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:27:40		
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:27:44	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:27:44		
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:27:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng

Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S 'IN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 Navigation cess ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:28:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12545	2020-09-09 01:28:49	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 A
Security	Audit Success	12545	2020-09-09 01:28:49	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1000 Account Name: defaultuser0 A
Security	Audit Success	12544	2020-09-09 01:29:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:29:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:29:27		
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:29:27	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:29:28		
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:29:28	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:29:28		

Navigation

Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:29:30	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:29:30		
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 01:29:40	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:29:40		
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:29:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:06	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:30:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:30:55	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:30:55		
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:30:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12544	2020-09-09 01:31:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng	
Security	Audit Success	12548	2020-09-09 01:31:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12544	2020-09-09 01:32:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng	
Security	Audit Success	12548	2020-09-09 01:32:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	13824	2020-09-09 01:32:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:32:33	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:32:59		
Security	Audit Success	13824	2020-09-09 01:32:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:32:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:33:00	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:33:00		
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:33:01	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:33:01		

Navigation

Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:33:01	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:33:01		

Navigation

Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:33:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	12544	2020-09-09 01:33:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:33:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\5ea8996c5812078b0dbb556f1303332e_970e8aca-7c00-49b
Security	Audit Success	12292	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\5a495a0c9b0a09c4c59f8f159fee4404_970e8aca-7c00-49ba-8584-67259f698fc7 Operation: %
Security	Audit Success	12292	2020-09-09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID

			01:33:52		

Navigation

Security	Audit Success	13824	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 01:33:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:33:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-09 01:33:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\5ea8996c5812078b0dbb556f1303332e_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-09 01:33:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\5a495a0c9b0a09c4c59f8f159fee4404_970e8aca-7c00-49ba-8584-67259f698fc7 Operation: %
Security	Audit Failure	12290	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Failure	12290	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0

Security	Audit Success	13824	2020-09-09 01:33:57	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-2 Navigation 02096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	12290	2020-09-09 01:33:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:33:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 01:33:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\5ea8996c5812078b0dbb556f1303332e_970e8aca-7c00-49b
Security	Audit Success	13824	2020-09-09 01:33:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 01:33:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 01:33:59	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	13824	2020-09-09 01:33:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:33:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 01:34:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:34:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID
Security	Audit Success	12292	2020-09-09 01:34:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\5ea8996c5812078b0dbb556f1303332e_970e8aca-7c00-49b
Security	Audit Success	12292	2020-09-09 01:34:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logon ID: 0x3e C:\ProgramData\Microsoft\Crypto\SystemKeys\5a495a0c9b0a09c4c59f8f159fee4404_970e8aca-7c00-49ba-8584-67259f698fc7 Operation: %
Security	Audit Success	12290	2020-09-09 01:34:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 01:34:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 01:34:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:34:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:34:02	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:34:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:34:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:34:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:34:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:34:03	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	13824	2020-09-09 01:34:10	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:34:10	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:34:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:34:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:34:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:34:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12544	2020-09-09 01:34:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:34:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:34:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:34:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12544	2020-09-09 01:34:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:34:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:34:52	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	12544	2020-09-09 01:34:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a

					fields indicate where a remote logon request originated. Workstation r Navigation le and may be left blank in some cases. The ir services have participated in this logon request. - Package name indic as used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:34:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:34:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:34:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:34:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:34:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:34:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:34:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:34:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-09 01:35:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:35:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:35:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:35:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:35:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:35:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:35:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:35:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:35:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 01:35:52	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:35:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:35:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:36:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:36:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 01:36:24	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:24	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 01:36:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:36:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:36:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:36:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:36:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-09 01:36:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:36:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

			01:36:32		
Security	Audit Success	13824	2020-09-09 01:36:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:36:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:36:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:36:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 01:38:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:38:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:38:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 01:38:07	Security-Auditing	

Navigation

Security	Audit Success	12544	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:40:22	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:40:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:40:23		
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09 01:40:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc
Security	Audit Success	13826	2020-09-09	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Accc

			01:40:38		
Security	Audit Success	12544	2020-09-09 01:40:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation IN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:40:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:40:49	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:40:49		

Navigation

Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:40:50	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:40:51		

Navigation

Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

Security	Audit Success	13824	2020-09-09 01:40:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation : WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:40:55	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			01:40:55		
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:40:57	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:40:58		
Security	Audit Success	13824	2020-09-09 01:40:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:40:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:40:59	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:41:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:41:02		
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:41:03	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:41:03		
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:41:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:41:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:41:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:41:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:41:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:41:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:41:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:41:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:41:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:41:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:41:56		
Security	Audit Success	13824	2020-09-09 01:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:42:27	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			01:42:27		
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:42:27	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:42:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGl Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:42:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:42:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] Navigation : WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:42:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	12544	2020-09-09 01:42:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:42:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:42:50	Microsoft-Windows-Security-Auditing	4726: A user account was deleted. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13826	2020-09-09 01:42:50	Microsoft-Windows-Security-Auditing	4733: A member was removed from a security-enabled local group. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-09 01:42:50	Microsoft-Windows-Security-Auditing	4729: A member was removed from a security-enabled global group. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1
Security	Audit Success	13826	2020-09-09 01:42:51	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:43:05		
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:43:06	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:43:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 01:43:31	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 01:43:32	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	12544	2020-09-09 01:44:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:44:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:45:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:45:01	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:45:01		
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:24	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:45:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:45:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		09 01:45:40	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:45:40		
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 01:45:40	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:45:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 01:45:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:45:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 01:45:45	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:45:45	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 01:46:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:46:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI

	Success		09 01:47:15	Security-Auditing	Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account o Navigation equested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:47:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:49:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:49:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:49:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:49:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 01:49:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 01:49:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 01:52:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:52:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai

	Success		09 01:52:53	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:53:00	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 01:53:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 01:53:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	12544	2020-09-09 01:56:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 01:56:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 01:56:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 01:56:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 01:56:08	Security-Auditing	
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			01:56:08		
					Navigation
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 01:56:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 02:00:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:00:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:00:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:00:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:00:30	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 02:00:30	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 02:05:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:05:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:05:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 02:05:38	Security-Auditing	

Navigation

Security	Audit Success	13826	2020-09-09 02:05:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 02:05:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 02:10:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:10:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:11:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:11:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:14:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:14:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:14:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:14:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:14:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:14:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:14:13	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	13826	2020-09-09 02:14:13	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acco
Security	Audit Success	12544	2020-09-09 02:14:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:14:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:15:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a

					fields indicate where a remote logon request originated. Workstation r Navigation le and may be left blank in some cases. The ir services have participated in this logon request. - Package name indic as used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:15:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:15:14	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	13826	2020-09-09 02:15:14	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Acc
Security	Audit Success	12544	2020-09-09 02:15:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:15:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGI Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2dc Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:15:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR

	Success		09 02:15:19	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 02:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:15:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WOR
Security	Audit Success	13824	2020-09-09 02:17:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	13824	2020-09-09 02:17:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domain: WORKGROUP Logor
Security	Audit Success	103	2020-09-09 02:18:22	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2020-09-09 02:18:22	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-09 02:18:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 02:18:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 02:18:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 02:18:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13824	2020-09-09 02:18:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: WIN-6IHPAH0E5VQ$ Account Domai
Security	Audit Success	13312	2020-09-09 02:18:39	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:39	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-09 02:18:39	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-09 02:18:39	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-09 02:18:40	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:40	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:42	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Security	Audit Success	12288	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE s system is initialized.
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwc which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x248 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x248 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0?????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0?????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit	13312	2020-09-	Microsoft-Windows-	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target

	Success		09 02:18:43	Security-Auditing	Process Command Line: ????0--?0??????????????????4 Token Eleva… e of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to s… n as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-09 02:18:43	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xae38
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is m on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is m on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 02:18:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-09 02:18:48	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.

Security	Audit Success	12544	2020-09-09 02:18:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:18:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:18:51	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 02:18:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3c096 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 02:18:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3c049 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-09 02:18:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-09 02:18:51	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13826	2020-09-09 02:18:52	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 02:18:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 02:18:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 02:18:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-09 02:18:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-09 02:18:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 02:18:55	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 02:18:55	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0

Security	Audit Success	12544	2020-09-09 02:18:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:18:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-09 02:18:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:18:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:18:56	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 02:18:56	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 02:19:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:19:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:19:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:19:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:19:02	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 02:19:02	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 02:19:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:19:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			02:19:04		

Navigation

Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 02:19:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:19:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:19:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-09 02:19:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:19:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-09 02:19:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:19:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:19:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 02:19:22	Security-Auditing	
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			02:19:22		
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:19:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Failure	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344 Navigation 96394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 02:19:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 02:19:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 02:19:46	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Contro
Security	Audit Success	12290	2020-09-09 02:19:52	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:19:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:19:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:19:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:20:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

	Success		09 02:20:01	Security-Auditing	

Navigation

Security	Audit Failure	12290	2020-09-09 02:20:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:20:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 02:20:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:20:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:20:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 02:20:14	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 02:20:14	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12290	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14d459 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce

			02:20:15		Length: 0 This event is generated when a logon session is created. It ıter that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logge dicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14d412 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2e4 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14ecd2 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14ec45 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	12548	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	13824	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-09 02:20:15	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		09 02:20:35	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			02:20:38		
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 02:20:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 02:20:40	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			02:20:41		
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 02:20:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L	

	Success		09 02:20:46	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:20:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:20:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:20:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:20:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:20:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:20:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:20:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:20:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:20:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:20:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:20:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 02:20:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 02:20:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 02:20:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:20:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:21:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i Navigation ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:21:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:24:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:24:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 02:24:36	Security-Auditing	
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			02:24:36		
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 02:25:48	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:25:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:29:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 02:29:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			02:29:13		
Security	Audit Success	12544	2020-09-09 02:32:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:32:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:33:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:33:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:33:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:33:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:33:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:33:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:33:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:33:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

			02:33:53		
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:33:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 02:42:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:42:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:43:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:43:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 02:45:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:45:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:46:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:46:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-09 02:55:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:55:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			02:55:56		
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 02:55:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-09 02:57:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 02:57:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			03:00:13		

Navigation

Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:00:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:00:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:00:30	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:00:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:00:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:00:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:00:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13826	2020-09-09 03:00:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do

Security	Audit Success	13826	2020-09-09 03:00:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S Navigation -18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 03:00:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 03:01:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:01:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:05:56	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

Security	Audit Success	13824	2020-09-09 03:05:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:05:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-09 03:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:06:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:07:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:07:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:07:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:07:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:07:08	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-09 03:11:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:11:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		09 03:12:30	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:12:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-09 03:12:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:12:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:12:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:12:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-09 03:18:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:18:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:18:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:18:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:18:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:18:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:21:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:21:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:25:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:25:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		09 03:25:56	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:25:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 03:27:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 03:27:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:27:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 03:27:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:27:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:27:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:27:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:27:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:28:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 03:28:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			03:28:49		
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:28:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 03:30:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:30:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:30:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:30:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:31:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:31:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 03:31:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L

	Success		09 03:34:05	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 03:34:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 03:34:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:34:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:37:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			03:37:17		
Security	Audit Success	12544	2020-09-09 03:38:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:38:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 03:38:09	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 03:38:09	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 03:41:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:41:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 03:42:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 03:42:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-09 17:51:11	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:11	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-09 17:51:11	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:11	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-09 17:51:11	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-09 17:51:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:14	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque

Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Secu Navigation Name: VIETHOANG$ Account Domain: WORK Process ID: 0x244 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit	13312	2020-09-	Microsoft-Windows-	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target

	Success		09 17:51:15	Security-Auditing	Process Command Line: ????0--?0???????????????e?????? Token Elev… …pe of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to s… …n as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-09 17:51:15	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb218
Security	Audit Success	101	2020-09-09 17:51:16	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is … on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s… intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is … on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s… intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a … fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in… services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su… indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers… have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su… indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers… have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su… indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers… have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su… indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers… have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su… indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers… have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica…
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su… indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers… have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica…

Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Secu Navigation Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System3 ormation: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19aa3 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x196ba Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	13824	2020-09-09 17:51:16	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12544	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 17:51:17	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			17:51:18		
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 17:51:18	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:51:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-09 17:51:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:51:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:51:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0

			17:51:23		
Security	Audit Success	12292	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 17:51:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-
Security	Audit Success	13824	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 17:51:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0

			17:51:28		
Security	Audit Success	12292	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x86955 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x8691b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:51:28	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2fc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event i
Security	Audit Success	12544	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x8a6ec Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is n KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which s
Security	Audit Success	12544	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x8a4ed Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is n KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which s
Security	Audit Success	12545	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

			17:51:29		
Security	Audit Success	12548	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ... ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whic ... among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:30		
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:31		
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 17:51:31	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:32		
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:51:33	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:33		
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:36		
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 17:51:36	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 17:51:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:38		
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 17:51:39	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:39		

Navigation

Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:51:39	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:39		Navigation
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		09 17:51:39	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:39		
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:51:39	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:51:39		
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 17:51:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:51:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:51:42	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 17:51:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Contro
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 17:51:48	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 17:51:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:51:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:52:11		

Navigation

Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 17:52:11	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:52:11		
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 17:52:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 17:52:12	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 17:52:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:52:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13824	2020-09-09 17:52:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Failure	12544	2020-09-09 17:52:17	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account (x86)\Microsoft\Edge\Application\msedge.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type f be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited se
Security	Audit Success	13824	2020-09-09 17:52:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 17:52:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:52:45	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:52:45		

Navigation

Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\88c968716b
Security	Audit Success	12292	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:52:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:52:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:52:48	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:52:48		
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:52:50	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:52:50		
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:52:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		09 17:53:12	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:53:13		

Navigation

Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:53:13	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:53:13		
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 17:53:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:53:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:53:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:53:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:53:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:53:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 17:53:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:53:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:53:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 17:53:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 17:57:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 17:57:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:57:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12548	2020-09-09 17:57:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			17:57:18		
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 17:57:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-09 17:57:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 17:57:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 17:57:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			17:57:20		
Security	Audit Success	12544	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x818 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x818 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x818 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x818 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x818 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 17:57:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12545	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 17:57:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se [illegible] nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 17:57:49	Security-Auditing	
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:57:49		

Navigation

Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-09 17:57:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-09 17:57:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	13824	2020-09-09 17:57:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 17:57:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x26f463 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L

	Success		09 19:41:29	Security-Auditing	Logon ID: 0x26f40d Network Account Name: - Network Account Dom 0000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It Navigation ter that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-09 19:41:29	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-09 19:41:30	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 19:41:30	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-09 19:41:30	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-09 19:41:30	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-09 19:41:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 19:41:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-09 19:41:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-09 19:41:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:46	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

Security	Audit Success	12544	2020-09-09 19:41:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] \ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:41:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 19:41:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:55	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 19:41:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:41:56		
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 19:41:56	Security-Auditing	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:41:56		
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:41:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		09 19:42:00	Security-Auditing	
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			19:42:00		
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:42:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 19:42:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 19:42:39	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 19:43:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		09 19:43:20	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 19:43:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:43:22		
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:43:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		09 19:43:25	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:43:26		
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:43:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 19:43:26	Security-Auditing	

Navigation

Security	Audit Success	12544	2020-09-09 19:45:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:45:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 19:47:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:47:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 19:47:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:47:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:47:15	Security-Auditing	servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f12 Navigation diting Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF servicingstack_31bf3856ad364e35_10.0.19041.441_none_e753a4f1261e4901\TiWorker.exe Auditing Settings: Original Security Descriptor: ?
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13826	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:47:16	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x5591ea Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack

Security	Audit Success	12544	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] \ETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x55919c Network Account Name: - Network Account Dom Navigation 0000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2fc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event i
Security	Audit Success	12544	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x55a96d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x55a7e7 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-09 19:48:22	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12290	2020-09-09 19:48:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 19:48:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-09 19:48:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			19:48:49		
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 19:48:50	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:48:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s

			19:49:52		that was accessed. The subject fields indicate the account on the local [illegible] the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i Navigation may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:49:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 19:49:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:49:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:49:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:49:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:49:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:49:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:49:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 19:53:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:53:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			19:55:13		

Navigation

Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:55:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-09 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:19	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:55:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

Navigation

	Success		09 19:56:32	Security-Auditing	
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:56:33		
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 19:56:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S -18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 19:57:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 19:58:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:58:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 19:58:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:58:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 19:58:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 19:58:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12545	2020-09-09 19:59:03	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		09 19:59:04	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 19:59:04	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:35		
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:35	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	Settings: Original Security Descriptor: ? New Security Descriptor: S:A[illegible] WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;S
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	Auditing Settings: Original Security Descriptor: ? New Security Descri[Navigation]f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Navigation

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Auditing Settings: Original Security Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:36	Security-Auditing	Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: ? New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)(AU;IDSAFA;0x1000000;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)(AU;IDSAFA;0x1000000;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)(AU;IDSAFA;0x1000000;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)(AU;IDSAFA;0x1000000;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)(AU;IDSAFA;0x1000000;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)(AU;IDSAFA;0x1000000;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:36		
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:36	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:37	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:37		
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:37	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:37		
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:37	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:37		
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:37	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:37		
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:37	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:38	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:38		
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:38	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:38		
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:38	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:38	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:39		
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:39	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:39		
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:39	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:39		
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:39	Security-Auditing	Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:39		
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:39	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:39		
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:39	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

Navigation

	Success		09 19:59:40	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Navigation

			19:59:40		
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:40	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:40		
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:40	Security-Auditing	S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:40		
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 19:59:40	Security-Auditing	Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUF New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			19:59:40		
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 19:59:40	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	103	2020-09-09 20:00:21	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-09 20:00:37	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:37	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-09 20:00:37	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:37	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-09 20:00:37	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-09 20:00:38	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:40	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inform 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	13312	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Security	Audit Success	13312	2020-09-09 20:00:41	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????e?????? Token Elev pe of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x240 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF

	Success		09 20:00:42	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	13568	2020-09-09 20:00:42	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb276
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 20:00:43	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:00:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:00:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 20:00:45	Security-Auditing	Navigation
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 20:00:45	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 20:00:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:00:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:00:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:00:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-09 20:00:47	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	13826	2020-09-09 20:00:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 20:00:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 20:00:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			20:00:49		
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID Navigation VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit	13568	2020-09-	Microsoft-Windows-	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP

	Success		09 20:01:00	Security-Auditing	Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL Ne Navigation \RAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:00	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

			20:01:01		
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Settings: Original Security Descriptor: S:AINO_ACCESS_CONTROL New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2020-09-09 20:01:01	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	12544	2020-09-09 20:01:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:01:05	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x7b4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 20:01:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x7f465 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 20:01:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x7f41d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-09 20:01:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-09 20:01:05	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-09 20:01:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 20:01:06	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		09 20:01:07	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:01:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-09 20:01:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:01:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 20:01:12	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 20:01:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:01:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:01:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:01:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:01:24	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

Navigation

Security	Audit Success	13824	2020-09-09 20:01:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:01:32	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:01:32		
Security	Audit Success	13824	2020-09-09 20:01:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

Security	Audit Success	12292	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Nam Navigation nt Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb917e6bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x7b4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x12cb03 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x12caa6 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x12e8f4 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x12e881 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	12548	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His

			20:01:36		
Security	Audit Success	13824	2020-09-09 20:01:36	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-09 20:01:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	13824	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:01:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi Navigation among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:01:55		
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:01:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:01:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:01:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			20:02:03		

Navigation

Security	Audit Success	13824	2020-09-09 20:02:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:02:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:02:06	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:02:06		
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:02:08	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:02:09		
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:02:20	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:02:21		
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:02:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-09 20:02:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:02:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 20:02:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 20:02:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 20:02:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:02:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:02:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:02:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:04:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:04:13	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:04:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:05:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:05:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:06:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:06:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [redacted] Navigation : LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:06:23	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:06:23		
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:06:25	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:06:27		
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-09 20:06:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		09 20:06:29	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:06:30		
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:06:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	12290	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344 Navigation 96394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\0864bb47
Security	Audit Success	12292	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-09 20:06:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:07:01	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:07:01		
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:07:03	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:07:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:07:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:07:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:07:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:07:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-09 20:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:11:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:11:09	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:11:09		
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:11:16	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:11:16		
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:11:17	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:11:17		
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:11:23	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-09 20:11:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:11:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			20:11:28		
Security	Audit Success	13824	2020-09-09 20:11:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:12:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:12:11	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:11		

Navigation

Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:12:11	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:11		
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:12:11	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:12		

Navigation

Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		09 20:12:12	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:12:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:13		
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:12:14	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:14		
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-09 20:12:15	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-09 20:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:16	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-09 20:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:12:17	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:17		
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:12:19	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:19		

Navigation

Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		09 20:12:19	Security-Auditing	
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:12:19		
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:12:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:15:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:15:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation 8718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:16:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:16:23	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-09 20:18:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:18:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:31:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:31:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		09 20:41:29	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 20:41:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 20:41:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:41:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:41:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:41:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 20:42:02	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 20:42:02	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 20:43:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-09 20:43:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:43:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-09 20:43:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:49:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:49:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 20:53:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 20:53:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 21:02:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:02:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 21:07:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:07:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Failure	12290	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-09 21:07:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-09 21:08:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:08:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-09 21:09:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-09 21:09:01	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723

Security	Audit Success	12292	2020-09-09 21:09:01	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-2334[illegible]96394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-09 21:11:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-09 21:15:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:15:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 21:15:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		09 21:15:43	Security-Auditing	
Security	Audit Success	12544	2020-09-09 21:15:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:15:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 21:16:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:16:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 21:21:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:21:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-09 21:21:34	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-09 21:21:34	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-09 21:35:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-09 21:35:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-09 21:36:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x370 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 21:36:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x370 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 21:36:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x370 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-09 21:36:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x370 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-09 21:36:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x370 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-09 21:36:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage

	Success		09 21:36:25	Security-Auditing	

Navigation

Security	Audit Success	12545	2020-09-09 21:36:26	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12544	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-09 21:36:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12545	2020-09-09 21:36:28	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-09 21:36:28	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	13824	2020-09-10 15:56:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x7b4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0

Security	Audit Success	12544	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [redacted] ETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xa6eaa1 Network Account Name: - Network Account Dom [redacted] 0000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xa6ea48 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13826	2020-09-10 15:56:56	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-10 15:56:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	12292	2020-09-10 15:56:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-[illegible]-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\M[illegible] Navigation cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-10 15:56:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-10 15:56:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:56:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-10 15:57:02	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 15:57:02	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 15:57:02	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-10 15:57:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 15:57:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 15:57:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 15:57:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 15:57:07	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0

			15:57:07		
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 15:57:08	Security-Auditing	
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			15:57:08		
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 15:57:08	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 15:57:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 15:57:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 15:57:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 15:57:12	Security-Auditing	
Security	Audit Success	13824	2020-09-10 15:57:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:57:13		
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 15:57:19	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:57:27		
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 15:57:27	Security-Auditing	
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:57:27		
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 15:57:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 15:57:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 15:57:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:57:37		

Navigation

Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		10 15:57:38	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 15:57:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:57:46		
Security	Audit Success	13824	2020-09-10 15:57:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:57:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 15:57:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-10 15:57:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 15:58:06	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12292	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x7b4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbc77ee Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbc77a8 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbc9433 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbc93cd Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit	12545	2020-09-	Microsoft-Windows-	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

	Success		10 15:58:19	Security-Auditing	
Security	Audit Success	12548	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12548	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID Hi
Security	Audit Success	13824	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 15:58:19	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID Hi
Security	Audit Success	13824	2020-09-10 15:58:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:58:38		

Navigation

Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		10 15:58:56	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 15:58:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

15:58:59

Navigation

Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:58:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:59:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 15:59:01	Security-Auditing	
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:59:01		
Security	Audit Success	13824	2020-09-10 15:59:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 15:59:02	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 15:59:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:59:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:59:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:59:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:59:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 15:59:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:02	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:00:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-10 16:01:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7
Security	Audit Success	12292	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7 Proce C:\ProgramData\Microsoft\Crypto\SystemKeys\586b219b37234f625694351842f5c9cd_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:02:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:02:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:02:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:02:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:02:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 16:02:15	Security-Auditing	
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			16:02:15		
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		10 16:02:18	Security-Auditing	
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			16:02:18		

Navigation

Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:02:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:06:57	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

Security	Audit Success	12544	2020-09-10 16:11:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:11:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:12:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		10 16:17:13	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:17:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:17:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:17:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:27:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s

			16:27:50		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:27:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:31:21	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-10 16:31:21	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-10 16:31:21	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-10 16:31:21	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	12544	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:31:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 16:35:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:35:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12544	2020-09-10 16:36:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:36:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:51:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:51:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:52:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 16:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 16:52:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-10 16:52:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:52:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do

Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S -18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 16:52:58	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-10 16:53:02	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 16:53:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 16:53:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	12544	2020-09-10 16:53:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:53:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:53:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			16:53:22		
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		10 16:53:23	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:53:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 16:57:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 16:58:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		10 16:58:23	Security-Auditing	
Security	Audit Success	12544	2020-09-10 16:58:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 16:58:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 17:02:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:02:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 17:02:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:02:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 17:07:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 17:08:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:08:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Failure	12290	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		10 17:08:01	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			17:08:02		

Navigation

Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 17:08:02	Security-Auditing	
Security	Audit Success	13824	2020-09-10 17:08:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			17:08:03		
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 17:15:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 17:15:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 17:15:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-10 17:15:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 17:15:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 17:15:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-10 17:19:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:19:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 17:21:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-10 17:21:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 17:25:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 17:25:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:25:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 17:25:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:25:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 17:26:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 17:26:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-10 17:26:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 17:35:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:35:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 17:36:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 17:36:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 17:40:46	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x23cc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-10 17:40:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23cc Process Name: C:\Windows\ the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 17:40:47	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x23cc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-10 17:40:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23cc Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 17:40:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23cc Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-10 17:40:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-10 17:40:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manage
Security	Audit Success	12544	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-10	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma

			17:40:49		

Navigation

Security	Audit Success	12545	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-2 Account Name: UMFD-2 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 17:40:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 18:19:46	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x7b4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-10 18:19:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x229c361 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 18:19:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x229c2a0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-10 18:19:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-10 18:19:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His

			18:19:46		
					Navigation
Security	Audit Success	12545	2020-09-10 18:19:48	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-10 18:19:48	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x658 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x658 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x658 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x658 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x658 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-4 Account Name: DWM-4 Account Domain: Window Manage

	Success		10 18:19:51	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-4 Account Name: DWM-4 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:19:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12292	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x7b4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x22b5ec7 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x22b5e7e Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi

					for whom the new logon was created, i.e. the account that was logged correlate this event with a KDC event. - Transited services indicate wh
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x22b65cc Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x22b6554 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Pro This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:19:56	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-10 18:19:56	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Failure	12290	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:19:59	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:19:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:19:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 18:20:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:20:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:20:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-3 Account Name: UMFD-3 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12545	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	13824	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:20:04	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:05	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Contr
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

			18:20:06		

Navigation

Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344 Navigation	96394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		10 18:20:06	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:07		
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 18:20:08	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:08		
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344 Navigation 96394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Failure		10 18:20:09	Security-Auditing	

Navigation

Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

			18:20:10		

Navigation

Security	Audit Failure	12290	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Contr
Security	Audit Success	13824	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:20:12	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:13		

Navigation

Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:20:13	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:15		

Navigation

Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:20:15	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:22		
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:20:22	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:22		

Navigation

Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		10 18:20:23	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:20:23		

Navigation

Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:20:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-10 18:20:26	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-10 18:20:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 18:20:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	103	2020-09-10 18:20:43	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-10 18:20:58	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:20:58	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-10 18:20:58	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:20:58	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-10 18:20:58	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-10 18:20:59	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Security	Audit Success	13312	2020-09-10 18:21:01	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: [redacted] - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Eleva e of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x240 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		10 18:21:02	Security-Auditing	Navigation
Security	Audit Success	12548	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	13312	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-10 18:21:02	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb1b4
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ` may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5b0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19243 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19001 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-10 18:21:03	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-10 18:21:04	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		10 18:21:05	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s Navigation that was accessed. The subject fields indicate the account on the local :he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 18:21:05	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-10 18:21:06	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-10 18:21:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:21:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-10 18:21:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:21:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	12544	2020-09-10 18:21:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:21:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:21:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12544	2020-09-10 18:21:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] IETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:21:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 18:21:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:21:15	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 18:21:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12292	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0

Security	Audit Success	12544	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Secu Navigation Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5b0 Process Name: C:\Windows\System3 ormation: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x98832 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x987e5 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x9a6cd Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12544	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x9a5b1 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12545	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:17		

Navigation

Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 18:21:17	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:17		

Navigation

Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 18:21:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:21:18	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:18		

Navigation

Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 18:21:18	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:18		

Navigation

Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:21:19	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:26	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 18:21:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:21:35	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:35		
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 18:21:35	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:35		
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:21:36	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:36		

Navigation

Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 18:21:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:21:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49l
Security	Audit Success	12292	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-10 18:21:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit	12292	2020-09-	Microsoft-Windows-	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

	Success		10 18:21:58	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:21:59		
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 18:22:00	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:22:00		

Navigation

Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:22:01	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:22:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 18:22:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:22:44		

Navigation

Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		10 18:22:44	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-10 18:22:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 18:22:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\88c968716b
Security	Audit Success	12292	2020-09-10 18:22:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-10 18:22:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:22:47		
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:22:47	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:22:48		
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		10 18:22:50	Security-Auditing	
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:22:50		
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:22:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 18:23:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:23:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:23:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:23:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:23:09	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-10 18:23:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 18:23:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:23:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		10 18:23:10	Security-Auditing	
Security	Audit Success	12544	2020-09-10 18:24:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:24:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:24:06	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 18:52:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:52:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:52:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:52:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 18:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:52:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:52:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12292	2020-09-10	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0

			18:52:52		
Security	Audit Success	12292	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5b0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x28fdd8 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x28fd93 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-10 18:52:52	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x291d30 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x291c69 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 18:52:53	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:52:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:52:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:52:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:52:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 18:52:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 18:52:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 18:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:53:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:53:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:53:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:53:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-10 18:54:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 18:54:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 18:54:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-10 18:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:54:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:54:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		10 18:54:49	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:54:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 18:58:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 18:58:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:58:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 18:59:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 18:59:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:09:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:09:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:09:58	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation t Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:09:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 19:12:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:12:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:14:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:14:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-10 19:20:20	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:20	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-10 19:20:20	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-10 19:20:20	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-10 19:20:21	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Security	Audit Success	13312	2020-09-10 19:20:22	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elev pe of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:24	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x244 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc

Security	Audit Success	12548	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-10 19:20:25	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb28e
Security	Audit Success	101	2020-09-10 19:20:26	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ` may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		10 19:20:28	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation :he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 19:20:28	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-10 19:20:29	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-10 19:20:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-10 19:20:29	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 19:20:29	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-10 19:20:30	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 19:20:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4

Security	Audit Success	12292	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Nam C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microso	nt Domain: NT AUTHORITY Logon ID: 0x3e5 F :b733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12544	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0	
Security	Audit Success	12544	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x7514b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack	
Security	Audit Success	12544	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x750fa Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack	
Security	Audit Success	12544	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2fc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event i	
Security	Audit Success	12544	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L ID: 0x757c5 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is r KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which s	
Security	Audit Success	12544	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L ID: 0x75790 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates	
Security	Audit Success	12545	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account	
Security	Audit Success	12545	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account	
Security	Audit Success	12548	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b	
Security	Audit Success	12548	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b	
Security	Audit Success	13824	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His	
Security	Audit Success	13824	2020-09-10 19:20:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His	
Security	Audit Success	13826	2020-09-10 19:20:43	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	12290	2020-09-10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	

			19:20:44		
Security	Audit Success	12292	2020-09-10 19:20:44	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-10 19:20:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-10 19:20:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 19:20:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 19:20:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-10 19:20:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-10 19:20:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:20:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:20:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:20:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:20:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13826	2020-09-10 19:20:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S -18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 19:20:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-10 19:20:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:20:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 19:20:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 19:20:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:20:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:21:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:21:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:21:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:21:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:21:01	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 19:21:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		10 19:21:09	Security-Auditing	
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:21:09		
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-10 19:21:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12290	2020-09-10 19:21:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 19:21:31	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 19:21:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:31	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 19:21:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:21:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 19:21:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-10 19:21:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:21:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:21:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13826	2020-09-10 19:21:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-10 19:21:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-10 19:22:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:22:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:22:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:22:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 19:22:22	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:22:23		
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		10 19:22:25	Security-Auditing	
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			19:22:25		
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 19:22:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		10 19:22:29	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation :he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:22:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:22:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:22:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:22:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:22:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:22:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:24:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:24:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:24:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\0864bb47f
Security	Audit Success	12292	2020-09-10 19:25:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0

Security	Audit Success	12544	2020-09-10 19:29:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] Navigation [illegible]ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible]x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:29:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:31:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 19:33:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:33:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s

			19:33:55		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:33:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:33:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:33:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:33:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:33:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:33:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:33:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 19:35:44	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:35:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 19:40:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 19:40:26	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-10 19:40:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 19:40:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-10 19:57:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 19:57:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 20:04:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		10 20:04:01	Security-Auditing	
Security	Audit Success	12544	2020-09-10 20:04:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:04:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 20:05:15	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:10:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 20:10:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:10:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 20:20:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:20:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 20:26:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 20:26:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:26:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 20:26:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Failure	12290	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:26:56		
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 20:26:57	Security-Auditing	
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:26:57		
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 20:26:57	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:26:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-10 20:26:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 20:26:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 20:26:58	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-10 20:35:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:35:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		10 20:40:32	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-10 20:40:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-10 20:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:49:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-10 20:50:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:50:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 20:52:08	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 20:52:08	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 20:52:08	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-10 20:55:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-10 20:55:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-10 20:58:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10 20:58:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 20:58:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-10 20:58:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-10 20:58:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-10	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723

			20:58:19		
Security	Audit Success	12292	2020-09-10 20:58:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-23344[illegible] Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-10 20:58:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-10 20:58:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x12ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x12ac Process Name: C:\Windows\ the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x12ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x12ac Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x12ac Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-10 20:59:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12545	2020-09-10 20:59:12	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12544	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			20:59:13		
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-10 20:59:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12545	2020-09-10 20:59:14	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-10 20:59:14	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	13824	2020-09-11 11:21:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xc8a7b2 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xc8a705 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 A[illegible] Navigation [illegible]$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13826	2020-09-11 11:21:44	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		11 11:21:48	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-11 11:21:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:21:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:53	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:21:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-11 11:21:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-11 11:21:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:21:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:21:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:21:59	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13824	2020-09-11 11:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:21:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:22:01	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 11:22:03	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:03		
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 11:22:05	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:05		
Security	Audit Success	13824	2020-09-11 11:22:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 11:22:10	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			11:22:10		

Navigation

Security	Audit Success	13824	2020-09-11 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 11:22:11	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:11		

Navigation

Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		11 11:22:12	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:22		

Navigation

Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		11 11:22:22	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:24		

Navigation

Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:22:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		11 11:22:26	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:22:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:26	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 11:22:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:27		

Navigation

Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 11:22:27	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:27		
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:22:31	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 11:22:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 11:22:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 11:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 11:22:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:22:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:22:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:23:00		
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 11:23:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		11 11:23:01	Security-Auditing	
Security	Audit Success	13824	2020-09-11 11:23:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			11:23:02		

Navigation

Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:23:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 11:24:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		11 11:24:43	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 11:24:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:24:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 11:26:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:26:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:26:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:26:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e8 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xe4602e Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xe45fe8 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce

			11:28:03		Length: 0 This event is generated when a logon session is created. It ıter that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logge dicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-11 11:28:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2fc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event i
Security	Audit Success	12544	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xe47cbd Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xe47c53 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-11 11:28:04	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		11 11:28:41	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:28:42		

Navigation

Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:28:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 11:33:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:33:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s

			11:36:48		that was accessed. The subject fields indicate the account on the local [Navigation] the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 11:36:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:36:49		
Security	Audit Success	13824	2020-09-11 11:36:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 11:36:50	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 11:36:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13312	2020-09-11 11:39:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:32	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-11 11:39:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-11 11:39:32	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-11 11:39:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\S

			11:39:36		the computer that was accessed. The subject fields indicate the accou ch requested the logon. This is most common network fields indicate where a remote logon request originated. Work s available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x244 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0?????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0?????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-11 11:39:36	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb285
Security	Audit Success	101	2020-09-11 11:39:37	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0

Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000(tion: Process ID: 0x2d4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage

	Success		11 11:39:37	Security-Auditing	Navigation
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		11 11:39:38	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-11 11:39:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 11:39:39	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit	13826	2020-09-	Microsoft-Windows-	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do

	Success		11 11:39:39	Security-Auditing	

Navigation

Security	Audit Success	12292	2020-09-11 11:39:40	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-11 11:39:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 11:39:40	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 11:39:40	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-11 11:39:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:39:41	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	12544	2020-09-11 11:39:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:39:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:39:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID:	SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:41:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12544	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-11 11:41:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12544	2020-09-11 11:41:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-11 11:41:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	13826	2020-09-11 11:41:45	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 11:41:45	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 11:41:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 11:41:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	12544	2020-09-11 11:42:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s	

			11:42:37		that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:42:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:42:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:43:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:43:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:43:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:43:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:43:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		11 11:43:55	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:43:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-11 11:49:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 11:49:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:49:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:49:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 11:49:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:49:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:49:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			11:49:43		

Navigation

Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13826	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 11:49:43	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-11 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 11:49:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:49:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			11:59:39		

Navigation

Security	Audit Success	13824	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:59:39	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 11:59:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 11:59:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 11:59:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:59:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:59:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 11:59:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 12:06:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:06:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 12:06:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:06:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 12:06:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 12:06:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4

Security	Audit Success	12292	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Nam C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microso	Navigation nt Domain: NT AUTHORITY Logon ID: 0x3e5 F :b733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12292	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0	
Security	Audit Success	12544	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5c0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0	
Security	Audit Success	12544	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14fba2d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack	
Security	Audit Success	12544	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14fb9f7 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack	
Security	Audit Success	12544	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2fc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event i	
Security	Audit Success	12544	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14fbf56 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind	
Security	Audit Success	12544	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x14fbf21 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind	
Security	Audit Success	12545	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account	
Security	Audit Success	12545	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account	
Security	Audit Success	12548	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E	
Security	Audit Success	12548	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E	
Security	Audit Success	13824	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His	
Security	Audit Success	13824	2020-09-11 12:17:24	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His	
Security	Audit Success	12544	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	

Security	Audit Success	12544	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [redacted] Navigation [redacted]ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [redacted]x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 12:17:25	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 12:17:26	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 12:17:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 12:17:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:17:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 12:17:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 12:17:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:17:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:17:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

			12:17:35		

Navigation

Security	Audit Success	12290	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 12:17:35	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 12:17:36	Security-Auditing	
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:17:36		
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 12:17:37	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 12:17:42	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-11 12:17:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:17:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:17:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 12:17:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:17:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:17:54		

Navigation

Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 12:17:57	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:17:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 12:18:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:18:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 12:18:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 12:18:20	Security-Auditing	
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:18:20		

Navigation

Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 12:18:20	Security-Auditing	
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:18:20		

Navigation

Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:18:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 12:18:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 12:18:31	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-11 12:18:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		11 12:18:38	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 12:19:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:19:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:19:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:19:43	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:27:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12544	2020-09-11 12:27:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:27:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:27:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:27:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 12:32:26	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 12:32:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 12:47:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:47:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 12:47:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:47:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 12:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:49:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:49:44		
Security	Audit Success	13824	2020-09-11 12:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 12:53:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:53:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			12:59:15		
Security	Audit Success	13824	2020-09-11 12:59:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 12:59:18	Security-Auditing	
Security	Audit Success	13824	2020-09-11 12:59:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:59:19		
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 12:59:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 12:59:21	Security-Auditing	
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			12:59:21		
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 12:59:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 13:09:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:09:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 13:09:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:09:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 13:15:21	Security-Auditing	
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:15:21		
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:15:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 13:18:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:18:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 13:19:39	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR

			13:19:44		

Navigation

Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 13:20:13	Security-Auditing	
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:20:13		

Navigation

Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 13:20:14	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 13:20:14	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:20:14	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 13:20:18	Security-Auditing	
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:20:18		

Navigation

Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 13:20:19	Security-Auditing	
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:20:19		

Navigation

Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 13:20:20	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:20:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 13:20:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:20:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 13:20:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:21:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-11 13:21:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	12290	2020-09-11 13:22:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 13:22:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-11 13:22:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-11 13:22:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 13:22:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:22:58	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		11 13:23:59	Security-Auditing	Navigation
Security	Audit Success	12290	2020-09-11 13:23:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 13:23:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:23:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 13:23:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-11 13:23:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 13:24:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:24:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 13:24:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 13:24:52	Security-Auditing	
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:24:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:24:52		
Security	Audit Success	12290	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:25:38	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Failure	12290	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 13:25:39	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:25:40		
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:25:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 13:27:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:27:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:31:46		
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:31:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 13:31:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:31:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 13:39:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:39:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 13:44:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:44:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 13:46:40	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 13:46:40	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		11 13:49:44	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 13:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 13:54:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:54:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 13:54:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 13:54:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 13:57:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 13:57:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 13:57:01	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:57:01	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 13:57:01	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 13:57:01	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			14:03:00		

Navigation

Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:03:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 14:03:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:03:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 14:03:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:03:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 14:07:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-11 14:07:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 14:09:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:09:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 14:17:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 14:17:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 14:17:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:17:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 14:17:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 14:17:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:19:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 14:25:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:25:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 14:32:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 14:32:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 14:32:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 14:32:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:32:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Failure	12290	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 14:32:36	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 14:32:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:32:37		
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 14:32:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Failure	12290	2020-09-11 14:32:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12544	2020-09-11 14:39:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-11 14:39:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12290	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0	
Security	Audit Success	12544	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x40e4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener	
Security	Audit Success	12544	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x40e4 Process Name: C:\Windows\ the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc	
Security	Audit Success	12544	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x40e4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener	
Security	Audit Success	12544	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x40e4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc	
Security	Audit Success	12544	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x40e4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc	
Security	Audit Success	12548	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage	
Security	Audit Success	12548	2020-09-11 14:40:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage	
Security	Audit Success	12545	2020-09-11 14:40:23	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma	
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s	

			14:40:25		that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 14:40:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 14:40:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 14:40:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:12:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5c0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x23e645a Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack

Security	Audit Success	12544	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x23e63ae Network Account Name: - Network Account Dor Navigation 00000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12545	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12548	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13826	2020-09-11 18:12:09	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

			18:12:11		
Security	Audit Success	12292	2020-09-11 18:12:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-11 18:12:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 18:12:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Failure	12544	2020-09-11 18:12:15	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x - Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Ne process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon
Security	Audit Success	12292	2020-09-11 18:12:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 18:12:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	13824	2020-09-11 18:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12292	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5c0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0

			18:12:19		
Security	Audit Success	12544	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x243f342 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x243f2fb Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2fc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event i
Security	Audit Success	12544	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x24405f9 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x244056a Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	12548	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	13824	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 18:12:19	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-11 18:12:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-11 18:12:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-11 18:12:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR

	Success		11 18:12:22	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 18:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:12:27	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 18:12:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:12:35		

Navigation

Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		11 18:12:36	Security-Auditing	
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:12:36		
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 18:12:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:12:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 18:12:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-11 18:12:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:12:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:12:56	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 18:12:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 18:12:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 18:12:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-11 18:13:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:13:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:13:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			18:13:40		

Navigation

Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 18:13:41	Security-Auditing	
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

			18:13:41		

Navigation

Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 18:13:42	Security-Auditing	
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:13:42		

Navigation

Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:13:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 18:13:44	Security-Auditing	
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:13:44		

Navigation

Security	Audit Success	13824	2020-09-11 18:13:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 18:13:45	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:13:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 18:14:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:14:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 18:14:20	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 18:14:20	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-11 18:14:20	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 18:22:10	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:22:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:22:41		

Navigation

Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 18:22:41	Security-Auditing	
Security	Audit Success	13824	2020-09-11 18:22:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:24:02		
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		11 18:24:03	Security-Auditing	
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:24:03		

Navigation

Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 18:24:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 18:24:05	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 18:24:05	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 18:24:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:24:35		

Navigation

Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 18:24:35	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:24:36		

Navigation

Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:24:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 18:24:37	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		11 18:25:16	Security-Auditing	Navigation
Security	Audit Success	12292	2020-09-11 18:25:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 18:25:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-11 18:25:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 18:25:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 18:25:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 18:25:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 18:25:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-11 18:27:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:27:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 18:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 18:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 18:27:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-11 18:31:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:31:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 18:38:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:38:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 18:38:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-11 18:38:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 18:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 18:59:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 18:59:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 18:59:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		11 18:59:21	Security-Auditing	
Security	Audit Success	12544	2020-09-11 19:04:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:04:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 19:04:15	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-11 19:04:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:04:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 19:04:17	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:17		
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 19:04:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:18		
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 19:04:18	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:18		
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 19:04:19	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:19		
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		11 19:04:20	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:21		
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 19:04:21	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:04:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:23		
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		11 19:04:25	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:04:25		

Navigation

Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:04:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12544	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12544	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	12548	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-11 19:04:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	12544	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	

	Success		11 19:08:20	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:08:21		

Navigation

Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 19:08:21	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 19:08:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:08:22		
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 19:08:22	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:08:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:12:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:26:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:26:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		11 19:35:53	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation :he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:35:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:35:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		11 19:38:00	Security-Auditing	Navigation
Security	Audit Success	12290	2020-09-11 19:38:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 19:38:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 19:38:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 19:38:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 19:38:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:42:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12544	2020-09-11 19:52:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] Navigation [illegible]ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible]x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:52:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:52:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:52:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 19:52:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 19:52:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11 19:52:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12548	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 19:54:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	103	2020-09-	Microsoft-Windows-	1100: The event logging service has shut down.

	Success		11 19:54:13	Eventlog	
Security	Audit Success	13312	2020-09-11 19:54:29	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:29	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-11 19:54:29	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:29	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-11 19:54:29	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-11 19:54:30	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x240 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12548	2020-09-11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			19:54:33		

Navigation

Security	Audit Success	12548	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-11 19:54:33	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb42e
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x197ca Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x195b3 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		11 19:54:34	Security-Auditing	

Navigation

Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-11 19:54:34	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 19:54:35	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 19:54:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-11 19:54:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-11 19:54:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 19:54:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 19:54:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-11 19:54:38	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-11 19:54:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:54:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			19:54:41		

Navigation

Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:54:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-11 19:54:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 19:54:44	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-11 19:54:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-11 19:54:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:54:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 19:54:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 19:54:49	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-11 19:54:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:54:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:54:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:54:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:54:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:55:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:55:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:55:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:55:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:55:01	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

Security	Audit Success	12290	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Accou Navigation Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xd9cb3 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xd9c6d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-11 19:55:03	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0xdb1c8 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12544	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0xdb162 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12545	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

			19:55:04		
Security	Audit Success	12545	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-11 19:55:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-11 19:55:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 19:55:10	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:55:10		
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 19:55:10	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:55:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:55:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:55:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:55:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 19:55:18	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:55:18		

Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 19:55:33	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:55:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:55:45		
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		11 19:55:45	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\88c968716b
Security	Audit Success	12292	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:55:48		
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 19:55:49	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 19:55:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:55:51		
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		11 19:55:52	Security-Auditing	
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:55:52		
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:55:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 19:55:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:55:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:55:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:55:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s

			19:56:46		that was accessed. The subject fields indicate the account on the local [redacted] the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i [redacted] may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:56:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:56:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:56:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 19:56:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:56:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 19:56:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 19:56:50	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-11 19:57:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:57:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:57:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:58:46	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] Navigation : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 19:59:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-11 20:02:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:02:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:03:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:03:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		11 20:05:01	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:05:01	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

	Success		11 20:09:36	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:09:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 20:09:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:09:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-11 20:09:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12544	2020-09-11 20:09:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:09:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation t Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:15:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		11 20:15:49	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:15:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 20:18:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:18:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 20:18:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 20:18:29	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 20:18:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 20:18:30	Security-Auditing	
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:18:30		

Navigation

Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 20:18:31	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:18:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-11 20:18:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 20:18:48	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0

			20:18:48		

Navigation

Security	Audit Success	13824	2020-09-11 20:20:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 20:20:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 20:20:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 20:20:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-11 20:20:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-11 20:21:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:21:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Failure	12290	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\a1a81b61
Security	Audit Success	12292	2020-09-11 20:21:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-11 20:24:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:24:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		11 20:24:44	Security-Auditing	
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:24:44		

Navigation

Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:24:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12544	2020-09-11 20:30:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:30:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:33:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:33:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:39:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 20:39:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:39:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 20:39:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:39:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 20:39:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:39:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 20:39:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation t Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 20:45:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 20:49:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:49:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:49:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:49:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:49:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:49:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 20:54:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 20:54:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s

			21:04:15		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		11 21:04:15	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-11 21:04:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:04:20	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-11 21:04:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:04:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 21:09:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:09:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 21:09:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:09:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			21:15:49		

Navigation

Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-11 21:15:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-11 21:24:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:24:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-11 21:27:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-11 21:27:15	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-11 21:37:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:37:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 21:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-11 21:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x514 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x514 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x514 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x514 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x514 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc

Security	Audit Success	12548	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] ne: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-11 21:40:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12544	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12548	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-11 21:40:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-11 21:40:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-11 21:40:25	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	12548	2020-09-11 21:40:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12545	2020-09-11 21:40:26	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-11 21:40:26	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	13824	2020-09-12 11:20:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-12 11:20:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:20:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:20:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x99ff6d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x99ff17 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	12548	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		12 11:20:48	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13826	2020-09-12 11:20:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-12 11:20:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:20:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-12 11:20:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 11:20:49	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:20:50	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Failure	12290	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:20:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 11:20:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:20:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:20:55		
Security	Audit Success	13824	2020-09-12 11:20:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:20:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:20:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:21:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:21:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:21:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:21:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:21:05	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:21:15	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:21:15		

Navigation

Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:21:15	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:21:15		

Navigation

Security	Audit Success	13824	2020-09-12 11:21:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		12 11:21:21	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 11:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:21:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 11:21:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:21:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:21:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:21:35	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:21:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 11:21:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:21:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 11:21:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12544	2020-09-12 11:21:37	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x Name: - Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Packa local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common ty provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in th
Security	Audit Success	12292	2020-09-12 11:21:37	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:21:37	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:21:41	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:21:41	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5d0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xac7ecb Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xac7e86 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2dc Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xac8e20 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce

			11:21:42		event is generated when a logon session is created. It is generated on [illegible] :cessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The netw Navigation remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0xac8dba Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:21:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-12 11:21:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:21:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:21:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-12 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-12 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-12 11:22:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU
Security	Audit Success	13824	2020-09-12 11:22:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROU

Security	Audit Success	13824	2020-09-12 11:22:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:22:10	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:10	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:12		

Navigation

Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		12 11:22:13	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:22:14		
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:22:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12290	2020-09-12 11:22:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344 Navigation	96394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:22:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:22:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.yourphone_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723dccff	
Security	Audit Success	12292	2020-09-12 11:22:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 11:22:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc	
Security	Audit Success	12292	2020-09-12 11:22:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 11:22:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:22:48	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc	
Security	Audit Success	12292	2020-09-12 11:22:48	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 11:22:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:22:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 11:22:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 11:22:51	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 11:22:51	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:22:51	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\a1a81b613	
Security	Audit Success	12292	2020-09-12 11:22:51	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 11:22:51	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 11:22:51	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12544	2020-09-12 11:23:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica	
Security	Audit Success	12548	2020-09-12 11:23:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log	
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI	

			11:23:47		

Navigation

Security	Audit Success	13824	2020-09-12 11:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:23:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:23:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:23:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:23:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:23:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:23:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 11:23:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:23:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:23:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:23:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:23:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:23:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:23:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:23:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:23:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:23:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:23:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:24:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			11:24:03		
Security	Audit Success	13824	2020-09-12 11:24:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:05	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:24:05	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:24:06	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:24:07		
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:24:07	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:24:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:25:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	103	2020-09-12 11:25:57	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-12 11:26:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:12	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-12 11:26:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.

Security	Audit Success	13312	2020-09-12 11:26:12	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: [redacted] - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Eleva e of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-12 11:26:12	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-12 11:26:13	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:15	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	13312	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:26:16	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x250 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x250 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2b4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b4 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s

			11:26:17		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	13568	2020-09-12 11:26:17	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb2e2
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2b4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2b4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x1f10b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0x1bbda Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: I
Security	Audit Success	13824	2020-09-12 11:26:19	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit	12292	2020-09-	Microsoft-Windows-	5033: The Windows Firewall Driver started successfully.

	Success		12 11:26:20	Security-Auditing	
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 11:26:20	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 11:26:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 11:26:21	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:26:21	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:26:22	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 11:26:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 11:26:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:26:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:26:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:26:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 11:26:30	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 11:26:30	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12544	2020-09-12 11:26:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

			11:26:31		
Security	Audit Success	12290	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x84ad9 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x84a86 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13826	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:26:31	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2ec Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x878d8 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th

					logon was created, i.e. the account that was logged on. The network f Navigation ote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate ser this logon request. - Package name indicates
Security	Audit Success	12544	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0x87865 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12545	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 11:26:32	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:26:33		
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:26:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:26:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:26:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:26:42	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 11:26:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:26:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:26:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:26:55		

Navigation

Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation	06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:26:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12290	2020-09-12 11:26:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:26:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c	
Security	Audit Success	12292	2020-09-12 11:26:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 11:27:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit	12292	2020-09-	Microsoft-Windows-	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain:	

	Success		12 11:27:01	Security-Auditing	C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8w[illegible]oft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 11:27:01	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:27:02		

Navigation

Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12290	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0	
Security	Audit Success	12290	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0	
Security	Audit Success	12290	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0	
Security	Audit Success	12292	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49	
Security	Audit Success	12292	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4	
Security	Audit	12292	2020-09-	Microsoft-Windows-	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0	

	Success		12 11:27:13	Security-Auditing	

Navigation

Security	Audit Success	12292	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			11:27:21		

Navigation

Security	Audit Success	13824	2020-09-12 11:27:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		12 11:27:24	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:27:24		
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:27:26	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:27:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:27:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:27:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:27:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:27:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

	Success		12 11:27:33	Security-Auditing	Navigation
Security	Audit Success	12290	2020-09-12 11:27:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:27:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:27:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:27:52	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:27:52	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:27:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:27:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:27:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:27:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:27:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13826	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:27:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-12 11:28:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12292	2020-09-	Microsoft-Windows-	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain:

	Success		12 11:28:13	Security-Auditing	C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_c oft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:28:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:28:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:28:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:28:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:28:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:29:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:29:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:29:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:29:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:30:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:30:03	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:30:03		

Navigation

Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:30:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:30:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:30:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Navigation

	Success		12 11:30:51	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:30:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:30:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:30:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:30:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:30:56	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:33:44		

Navigation

Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		12 11:33:46	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:33:46		

Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7
Security	Audit Success	12292	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4ecf03c26e8df7f8523c1a8f928b030b_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7 Proce C:\ProgramData\Microsoft\Crypto\SystemKeys\b1e0768a3091627204a208d86f9cc86d_970e8aca-7c00-49ba-8584-67259f698fc7 Operation:
Security	Audit Success	12292	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x3e7
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:33:51	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:33:51		

Navigation

Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:33:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:36:42	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:36:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:36:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:37:46	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 11:37:47	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:37:47	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12292	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Additional Information: localhost Process Information: Process ID: 0x25d0 Process Name: C:\Program Files (x86)\Microsoft\Edge\Application\
Security	Audit Success	12544	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: be MicrosoftAccount Logon ID: 0x31421d Linked Logon ID: 0x31425b Network Account Name: - Network Account Domain: - Logon GUID: {0000 Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is ger

					(interactive) and 3 (network). The New Logon fields indicate the accou n was created, i.e. the account that was logge logon request. - Logon GUID is a unique identifier that can be used to a KDC event. - Transited services indicate whi
Security	Audit Success	12544	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: be MicrosoftAccount Logon ID: 0x31425b Linked Logon ID: 0x31421d Network Account Name: - Network Account Domain: - Logon GUID: {0000 Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is ger (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logge logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate whi
Security	Audit Success	12545	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 11:37:50	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accou Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User
Security	Audit Success	13824	2020-09-12 11:38:45	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:39:33	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 11:39:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:39:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:39:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:39:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit	12292	2020-09-	Microsoft-Windows-	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Navigation

	Success		12 11:39:35	Security-Auditing	Return Code: 0x0
Security	Audit Success	13824	2020-09-12 11:39:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:39:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:39:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:39:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOI
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:49:41		
Security	Audit Success	13824	2020-09-12 11:49:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Failure	12544	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x Name: - Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Packa local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common t provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in th
Security	Audit Success	12292	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:49:44		
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:49:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:49:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2e0 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:49:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12292	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e4 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3d941b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3d9371 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b

Security	Audit Success	13824	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 A[illegible] Navigation $ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 11:49:49	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2ec Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3db565 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x3db4f9 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 11:49:50	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:49:54	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 11:50:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	12290	2020-09-12 11:50:05	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-2334[illegible]96394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:50:05	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:50:05	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:50:05	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:50:05	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:50:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:50:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:50:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:50:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:50:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:50:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12545	2020-09-12 11:50:43	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:50:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	103	2020-09-	Microsoft-Windows-	1100: The event logging service has shut down.

	Success		12 11:51:15	Eventlog	
Security	Audit Success	13312	2020-09-12 11:51:31	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:31	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-12 11:51:31	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:31	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-12 11:51:31	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-12 11:51:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x244 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a

					fields indicate where a remote logon request originated. Workstation r [Navigation] le and may be left blank in some cases. The ir services have participated in this logon request. - Package name indic as used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2a8 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2a8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc

					used when User Account Control is enabled and the user chooses to st Navigation n as administrator. An elevated token is also u application does not require administrative privilege, and the user doe rogram using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-12 11:51:35	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb26b
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5dc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x1a26d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19c04 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			11:51:36		

Navigation

Security	Audit Success	12548	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	12548	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:51:36	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:51:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do

			11:51:38		
Security	Audit Success	13826	2020-09-12 11:51:38	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-12 11:51:39	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-12 11:51:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:51:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:51:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 11:51:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i Navigation ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 11:51:47	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:51:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s

			11:51:50		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:51:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 11:51:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:51:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:51:59	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:52:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:52:07	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:52:07		

Navigation

Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 11:52:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:52:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:52:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:52:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 11:52:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:52:29	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			11:52:38		
Security	Audit Success	13824	2020-09-12 11:52:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		12 11:52:41	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:52:41		

Navigation

Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:52:43	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:52:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-12 11:52:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:52:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:52:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:52:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:53:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:53:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit	12292	2020-09-	Microsoft-Windows-	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		12 11:53:06	Security-Auditing	Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5dc Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x169c6f Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x169c28 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2e4 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x16ad66 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x16ac52 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatior event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

Security	Audit Success	12548	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible]6551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 11:53:39	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12290	2020-09-12 11:53:41	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:53:41	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:53:41	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:53:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:53:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:53:44	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:53:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:53:45		
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 11:53:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12290	2020-09-12 11:53:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 11:53:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:53:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 11:53:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 11:53:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1	
Security	Audit Success	12292	2020-09-12 11:53:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 11:53:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 11:53:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 11:53:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	13826	2020-09-12 11:53:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit Success	13826	2020-09-12 11:53:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do	
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L	

	Success		12 11:54:11	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ...x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local ...he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:11	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-12 11:54:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se[illegible]nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 11:54:27	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:54:27		

Navigation

Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 11:54:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 11:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 11:54:33	Security-Auditing	
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			11:54:33		

Navigation

Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 11:54:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:55:06	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:55:07	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:55:07	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 11:55:07	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:55:16	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:55:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723

Security	Audit Success	12292	2020-09-12 11:55:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-23344 Navigation 96394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 11:55:21	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12290	2020-09-12 11:55:31	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:55:31	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:55:31	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 11:55:32	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 11:55:32	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 11:55:32	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 11:55:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 11:55:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 11:55:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:01:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 12:05:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:05:04	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 12:05:04	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 12:05:10	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:05:10	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:05:10	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 12:05:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:05:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:05:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 12:05:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:05:12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:05:12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12548	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 12:06:39	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 12:06:40	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:06:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 12:07:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:07:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13826	2020-09-12 12:07:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S -18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 12:07:48	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 12:11:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:11:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 12:14:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:14:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 12:14:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 12:14:19	Security-Auditing	
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:14:19		
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 12:14:19	Security-Auditing	
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			12:14:19		
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 12:14:20	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:14:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-12 12:14:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 12:14:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc

			12:14:23		
Security	Audit Success	12292	2020-09-12 12:14:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-23344[illegible]-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:14:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\0864bb47f
Security	Audit Success	12292	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 12:17:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 12:17:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 12:17:13	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc

Security	Audit Success	12292	2020-09-12 12:17:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-23344 Navigation 96394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 12:21:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:21:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:24:16	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 12:31:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		12 12:31:49	Security-Auditing	
Security	Audit Success	12544	2020-09-12 12:36:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:36:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 12:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 12:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 12:54:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 12:54:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 12:54:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 13:06:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:06:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 13:06:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:06:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 13:06:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:06:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 13:06:43	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:06:43	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.photos_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:06:43	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 13:18:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:18:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 13:18:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:18:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 13:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:18:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12544	2020-09-12 13:18:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] \ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:18:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 13:18:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

			13:18:35		
Security	Audit Success	13824	2020-09-12 13:18:35	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 13:18:37	Security-Auditing	
Security	Audit Success	13824	2020-09-12 13:18:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:18:38		

Navigation

Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 13:18:38	Security-Auditing	
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:18:38		

Navigation

Security	Audit Success	13824	2020-09-12 13:18:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 13:18:40	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 13:18:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 13:18:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:18:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:18:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:18:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:18:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:18:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 13:18:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:18:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:18:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:18:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:18:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 13:18:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 13:18:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:18:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:18:48	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:18:48	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:18:48	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:18:48	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 13:21:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 13:21:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 13:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:26	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 13:21:27	Security-Auditing	
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:21:27		
					Navigation
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 13:21:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:21:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.minecraftuwp_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b3b69fa5ad
Security	Audit Success	12292	2020-09-12 13:21:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 13:21:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 13:21:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 13:21:38	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:38	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			13:21:39		

Navigation

Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:21:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		12 13:21:43	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 13:21:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:21:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:24:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 13:24:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 13:24:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 13:24:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 13:28:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:28:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	12290	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344[illegible]96394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\6429026c1
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 13:28:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L

	Success		12 13:29:01	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation :he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:29:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:29:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:29:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:30:30	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	12544	2020-09-12 13:30:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		12 13:30:33	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 13:30:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	13824	2020-09-12 13:30:43	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHC
Security	Audit Success	12290	2020-09-12 13:30:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 13:30:56	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.minecraftuwp_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b3b69fa5ad
Security	Audit Success	12292	2020-09-12 13:30:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 13:35:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:35:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 13:49:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:49:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 13:49:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			13:49:12		
Security	Audit Success	12544	2020-09-12 13:51:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 13:51:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 13:51:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:51:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 13:51:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 13:51:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 13:54:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:54:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 13:54:18	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 13:54:18	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 13:56:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 13:56:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:00:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:00:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 14:03:03	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:03:03	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 14:03:03	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:06		
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:06	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 14:03:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 14:03:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 14:03:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 14:03:07	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 14:03:08	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12290	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:03:09	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			14:03:09		
Security	Audit Success	12290	2020-09-12 14:03:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:03:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 14:03:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Failure	12290	2020-09-12 14:03:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:03:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:03:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:03:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:03:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 14:05:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:05:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		12 14:08:49	Security-Auditing	

Navigation

Security	Audit Success	12290	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:08:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 14:21:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:21:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:21:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:21:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 14:24:11	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:24:11	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 14:24:11	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		12 14:24:17	Security-Auditing	Navigation
Security	Audit Success	12292	2020-09-12 14:24:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:24:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 14:24:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:24:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 14:24:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:24:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:24:56	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723

Security	Audit Success	12292	2020-09-12 14:24:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-2334[illegible]96394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:24:56	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:24:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Failure	12290	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b0e870aa6
Security	Audit Success	12292	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:24:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 14:25:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:25:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:26:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:26:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:31:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:31:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		12 14:31:53	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:31:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 14:47:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:47:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:47:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:47:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:47:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:47:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 14:47:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 14:47:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:47:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:47:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 14:47:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 14:47:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 14:47:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 14:47:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 14:47:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 14:51:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:51:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:51:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:51:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:53:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:53:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 14:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers
have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:03:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:03:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:03:34	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-12 15:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 15:06:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 15:06:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s

			15:06:36		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:06:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:06:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:06:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:21:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:21:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:21:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 15:21:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 15:21:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 15:21:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 15:21:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:21:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 15:21:43	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	12544	2020-09-12 15:21:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] \ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:21:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:21:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:21:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			15:24:24		
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:24:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 15:28:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 15:28:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:28:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 15:28:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:36:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:36:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:36:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:36:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:42:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:42:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 15:44:29	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 15:44:29	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 15:44:29	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

			15:44:39		
Security	Audit Success	12292	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\0864bb47f
Security	Audit Success	12292	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 15:44:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 15:45:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 15:45:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 15:45:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 15:45:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:45:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:47:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:47:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:51:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:51:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:51:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 15:51:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers
have participated in this logon request. - Package name indicates whi Navigation among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 15:54:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 15:58:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 15:58:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 15:58:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 15:58:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 15:58:01	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 15:58:01	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0

			15:58:01		
Security	Audit Success	12292	2020-09-12 15:58:01	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 15:58:01	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 15:58:02	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 15:58:02	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 15:58:02	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:01:14	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:01:14	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:01:14	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:01:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:01:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:01:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

Security	Audit Success	12292	2020-09-12 16:01:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-[illegible] Navigation [illegible]-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:01:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:01:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:01:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:01:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.microsoft3dviewer_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb17
Security	Audit Success	12292	2020-09-12 16:01:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 16:01:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:01:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:27	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:28	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:01:35	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit	13824	2020-09-	Microsoft-Windows-	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

	Success		12 16:02:53	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 16:02:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:02:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:04:10	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12290	2020-09-12 16:05:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:05:13	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:05:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:05:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:05:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:05:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:05:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:05:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:05:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:06:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:06:34	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:06:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:06:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:06:34	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:06:34	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:06:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:06:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0

			16:06:35		
Security	Audit Success	12290	2020-09-12 16:06:36	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:06:36	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:06:36	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 16:06:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:06:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 16:06:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:06:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:06:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:06:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:06:48	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:06:48	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:08:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:08:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:08:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:08:52	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:08:52	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:08:52	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:08:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:08:52	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:08:52	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		12 16:08:53	Security-Auditing	Navigation
Security	Audit Success	12292	2020-09-12 16:08:53	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:08:53	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:53	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:09:54	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:09:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:09:55	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:09:55	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:09:55	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:09:55	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:11:41	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 16:11:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 16:11:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:11:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:11:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:11:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 16:14:51	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:14:51	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:14:51	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12545	2020-09-12 16:14:54	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12544	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d4 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			16:14:55		
					Navigation
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:14:55	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	103	2020-09-12 16:15:11	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-12 16:15:23	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:23	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-12 16:15:23	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-12 16:15:23	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-12 16:15:24	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:24	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0???????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x248 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x248 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s

			16:15:27		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-12 16:15:27	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb338
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The in services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is n on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in so intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Wi

			16:15:28		generated on the computer that was accessed. The subject fields indic :al system which requested the logon. This is r on. The network fields indicate where a remote logon request originat ot always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is r on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19a25 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x1972a Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage

			16:15:28		

Navigation

Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	13824	2020-09-12 16:15:28	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 16:15:29	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		12 16:15:30	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do

			16:15:30		

Navigation

Security	Audit Success	13826	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 16:15:30	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-12 16:15:31	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-12 16:15:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:15:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 16:15:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 16:15:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:15:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-12 16:15:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 16:15:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 16:15:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su

					indicate where a remote logon request originated. Workstation name i ' may be left blank in some cases. The impers have participated in this logon request. - Package name indicates whi among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:15:36	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 16:15:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:15:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit	12292	2020-09-	Microsoft-Windows-	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain:

	Success		12 16:15:40	Security-Auditing	C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_c Navigation oft\Crypto\TokenBindingKeys\Keys\b0e870aa6
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\0864bb47f
Security	Audit Success	12292	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 16:15:40	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			16:15:41		

Navigation

Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:41	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:42	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 16:15:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:15:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:15:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:15:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

			16:15:51		
Security	Audit Success	13824	2020-09-12 16:15:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:15:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 16:16:01	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 16:16:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 16:16:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 16:16:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:16:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 16:16:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 16:16:23	Security-Auditing	
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			16:16:23		
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 16:16:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 16:16:40	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	12544	2020-09-12 16:16:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:16:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 16:16:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 16:16:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-12 16:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			16:16:49		
Security	Audit Success	13824	2020-09-12 16:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12290	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\88c968716b
Security	Audit Success	12292	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 16:16:52	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:53	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			16:16:54		
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		12 16:16:55	Security-Auditing	
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			16:16:55		
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:16:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 16:17:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:17:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:17:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:17:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:17:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:17:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:17:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:17:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 16:17:38	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:17:38	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:17:38	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:17:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12292	2020-09-	Microsoft-Windows-	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain:

	Success		12 16:17:39	Security-Auditing	C:\Users\bebos\AppData\Local\Packages\microsoft.yourphone_8weky[illegible]rypto\TokenBindingKeys\Keys\cf5cb1723dccff
Security	Audit Success	12292	2020-09-12 16:17:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\f7bb91786bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x24095f Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x240918 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2e4 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x24225b Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proc This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x2421f2 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account

Security	Audit Success	12545	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233 Navigation 2096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 16:18:56	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12544	2020-09-12 16:22:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:22:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:22:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-233448718-3606551
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 16:24:40	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:24:40	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:12	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:13	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:14	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:25:14	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:14	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:14	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:14	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 16:25:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12548	2020-09-12 16:25:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: [illegible] Navigation SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 16:25:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 16:25:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-12 16:25:51	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:51	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:25:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:25:51	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 16:26:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:26:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:26:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 16:26:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:27:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 16:28:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:28:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 16:28:41	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:28:41	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:28:41	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 16:28:43	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:28:43	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 16:28:43	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s

			16:29:12		that was accessed. The subject fields indicate the account on the local [Navigation] the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i [Navigation] may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:29:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

			16:29:13		
Security	Audit Success	13824	2020-09-12 16:29:16	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:29:16	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:29:22	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 16:30:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:30:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:30:30	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

	Success		12 16:30:30	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 16:30:30	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 16:30:30	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 16:32:29	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:32:29	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:32:29	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:33:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:33:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:33:25	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:34:37	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:34:37	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:34:37	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:35:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:35:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:35:18	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation nt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:36:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 16:36:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:36:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:36:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:36:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 16:37:16	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 16:37:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 16:37:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12544	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:45:12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		12 16:45:12	Security-Auditing	

Navigation

Security	Audit Success	12544	2020-09-12 16:45:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:45:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:45:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:45:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:45:17	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 16:45:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 16:45:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 16:45:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:45:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:51:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:51:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 16:51:54	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 16:51:54	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 16:52:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 16:52:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:52:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 16:52:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	12544	2020-09-12 16:53:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:53:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:58:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:58:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 16:59:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	12544	2020-09-	Microsoft-Windows-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo

	Success		12 17:01:34	Security-Auditing	Logon GUID: {00000000-0000-0000-0000-000000000000} Process I x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local Navigation he logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:01:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 17:03:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:03:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 17:06:41	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12290	2020-09-12 17:10:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 17:10:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 17:10:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 17:10:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 17:12:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:12:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s

			17:15:50		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:15:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible] : VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:18:17	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 17:18:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 17:18:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.photos_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 17:18:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 17:18:23	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 17:18:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:18:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 17:25:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:25:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 17:25:34	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			17:25:35		
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 17:25:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 17:26:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:26:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 17:27:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:27:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 17:27:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:27:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 17:27:35	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 17:27:35	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 17:27:35	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 17:27:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 17:27:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			17:27:38		
Security	Audit Success	12548	2020-09-12 17:27:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 17:27:38	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 17:27:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 17:27:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 18:46:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 18:46:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 18:46:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 18:46:09	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 18:46:11	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 18:46:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 18:46:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 18:46:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:21	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 18:46:22	Security-Auditing	
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:46:22		
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:22	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 18:46:23	Security-Auditing	
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:46:23		

Navigation

Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:46:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 18:46:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x5e0 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbfa233 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbfa1ec Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His

Security	Audit Success	13824	2020-09-12 18:47:02	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Acc Navigation Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2e4 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xbfd62f Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo ID: 0xbfd5c3 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Info is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on th logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation nar with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates
Security	Audit Success	12545	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: E
Security	Audit Success	13824	2020-09-12 18:47:03	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 18:47:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 18:47:13	Security-Auditing	
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			18:47:13		

Navigation

Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:47:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 18:47:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 18:47:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\a1a81b61
Security	Audit Success	12292	2020-09-12 18:47:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 18:47:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 18:47:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 18:47:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 18:47:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 18:47:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 18:47:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 18:53:48	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 18:53:48	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 18:53:48	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 18:53:49	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 18:53:49	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 18:53:49	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 18:53:51	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 18:53:51	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 18:53:51	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0

Security	Audit Success	12544	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:56:11	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 18:56:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 18:56:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI

			18:56:12		
Security	Audit Success	13824	2020-09-12 18:56:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	12544	2020-09-12 19:02:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:02:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:02:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:02:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:05:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:05:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12545	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12548	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:06:44	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		12 19:06:44	Security-Auditing	Navigation
Security	Audit Success	103	2020-09-12 19:07:15	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	13312	2020-09-12 19:07:31	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a fu to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administra does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:31	Microsoft-Windows-Security-Auditing	4696: A primary token was assigned to process. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Proces
Security	Audit Success	13312	2020-09-12 19:07:31	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target 0??????? Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control polic the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:31	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13573	2020-09-12 19:07:31	Microsoft-Windows-Security-Auditing	4826: Boot Configuration Data loaded. Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 General Settings Launch Type: %%1848 HyperVisor Debugging: %%1843
Security	Audit Success	13312	2020-09-12 19:07:32	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0????????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:33	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	12288	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Inforn 0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: ? Network Information: Workstation Name: - Source Netwo which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.e available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was reque
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Windows\S the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoco
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x248 Process Name: C:\Windows\System32\wininit.exe Network Information: Network Address: - Port: - This event is generate
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x248 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica

Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [redacted] ETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000 Navigation cess ID: 0x2d8 Process Name: C:\Windows\S computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The ir services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key leng
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x2ac Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is genera
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2ac Process Name: C:\Wi generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHOF
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUT
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13312	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Elevation Type indicates the type of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Security	Audit Success	13312	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: [redacted] - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4 Token Eleva e of token that was assigned to the new proce used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????????4? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13312	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4688: A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: - Account Domain: - Logon ID: 0x3e7 Target Process Command Line: ????0--?0??????????????e?????? Token Elevation Type indicates the type of token that was assigned to the new proc used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also u application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
Security	Audit Success	13568	2020-09-12 19:07:34	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb4bb
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x594 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x1a30a Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x19c45 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proces Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12548	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

			19:07:35		
					Navigation
Security	Audit Success	12548	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	13824	2020-09-12 19:07:35	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	12292	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		12 19:07:36	Security-Auditing	Navigation
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 19:07:36	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-20 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

Security	Audit Success	13826	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S -18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 19:07:37	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12292	2020-09-12 19:07:38	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2020-09-12 19:07:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:07:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 %%2464 Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:07:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 19:07:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s

			19:07:45		that was accessed. The subject fields indicate the account on the local Navigation the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 19:07:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 19:07:46	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 19:07:47	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:07:49	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:07:49		
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:07:50	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:07:50		
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:07:50	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:07:50		
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:07:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:07:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:07:58	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12544	2020-09-12 19:07:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:07:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:08:03	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:04	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:07	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:08:08	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:08:08		
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:08:08	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:08:08		

Navigation

Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:08	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:08:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:08:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 19:08:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:08:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 19:08:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

	Success		12 19:08:28	Security-Auditing	

Navigation

Security	Audit Success	12292	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\23b4c56b9ca1860f77e2f496562aeef8_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12292	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\14f1df51f6024f5dee3af610d4effbbc_970e8aca-7c00-49
Security	Audit Success	12292	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\51bf81bc327ced4a6197ff1619e4a04c_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:28	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:08:29		
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:08:29	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:08:30		

Navigation

Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Failure	12544	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	4625: An account failed to log on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x Name: - Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Packa local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common ty provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in th
Security	Audit Success	12290	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0
Security	Audit Success	12290	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0

Security	Audit Success	12292	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Nam Navigation nt Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microso bf0b8cd3e50409156082f7b_970e8aca-7c00-4
Security	Audit Success	12292	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 F C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\4209eaffdcb733886bd5d690120742e5_970e8aca-7c00-
Security	Audit Success	12292	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 19:08:39	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12544	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x594 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x169c03 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x169bbd Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2e4 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x16b56d Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the ac the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Worksta event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0x16b4cb Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b

			19:08:42		
Security	Audit Success	12548	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: t
Security	Audit Success	13824	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 19:08:42	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 19:08:47	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 19:08:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:56	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:57	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 19:08:58	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:08:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:09:00		
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:09:02	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:09:02		

Navigation

Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:09:02	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 19:09:12	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:09:12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:09:12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:09:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:09:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:09:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:09:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 19:09:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:09:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0

			19:09:17		
					Navigation
Security	Audit Success	12290	2020-09-12 19:09:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:09:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:09:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:09:20	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:09:20	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:09:20	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:09:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:09:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:09:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:09:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:09:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:09:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:09:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:09:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:09:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 19:09:44	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 19:09:44	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12544	2020-09-12 19:10:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit	12548	2020-09-	Microsoft-Windows-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log

	Success		12 19:10:35	Security-Auditing	
Security	Audit Success	12544	2020-09-12 19:10:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:10:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:11:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:11:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:18	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

	Success		12 19:11:23	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 19:11:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:11:28	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:17:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:17:58	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 19:17:58	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 19:17:58	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 19:18:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:18:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 19:18:41	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 19:18:41	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-12 19:19:19	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:19:19	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:19:19	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:19:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:19:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:19:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:19:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:19:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:19:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:19:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:19:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0

			19:19:23		
					Navigation
Security	Audit Success	12290	2020-09-12 19:21:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:21:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:21:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:21:21	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:21:21	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:21:21	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:21:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:21:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:21:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:21:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:21:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:21:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:22:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:22:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:22:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:22:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:22:27	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b0e870aa6
Security	Audit Success	12292	2020-09-12 19:22:27	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:22:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:22:28	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:22:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b0e870aa6

Security	Audit Success	12292	2020-09-12 19:22:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-23344 Navigation 96394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:22:28	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:22:28	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:22:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12290	2020-09-12 19:23:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-2334[illegible]96394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:23:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:23:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:23:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:23:23	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:23:23	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:32:24		
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:24	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 19:32:25	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:32:25		
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:32:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12290	2020-09-12 19:32:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 19:32:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c	
Security	Audit Success	12292	2020-09-12 19:32:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 19:32:27	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 19:32:37	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 19:32:37	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c	
Security	Audit Success	12292	2020-09-12 19:32:37	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 19:33:42	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 19:33:42	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc	
Security	Audit Success	12292	2020-09-12 19:33:42	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 19:33:45	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	

	Success		12 19:33:45	Security-Auditing	Navigation
Security	Audit Success	12292	2020-09-12 19:33:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\0864bb47f
Security	Audit Success	12292	2020-09-12 19:33:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:33:45	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:33:45	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:33:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:33:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:33:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5381: Vault credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Accoun
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:34:36		
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 19:34:37	Security-Auditing	
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:34:39		
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:34:39	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	12290	2020-09-12 19:34:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 19:34:46	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 19:34:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.xboxgamingoverlay_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b3b69	
Security	Audit Success	12292	2020-09-12 19:34:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 19:34:46	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.xboxgamingoverlay_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b3b69	
Security	Audit Success	12292	2020-09-12 19:34:46	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Success	12290	2020-09-12 19:34:54	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 19:34:54	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc	
Security	Audit Success	12292	2020-09-12 19:34:54	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0	
Security	Audit Failure	12290	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Failure	12290	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	

	Success		12 19:34:55	Security-Auditing	Navigation
Security	Audit Success	12292	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\a0984c619
Security	Audit Success	12292	2020-09-12 19:34:55	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Failure	12290	2020-09-12 19:34:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 19:34:56	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:34:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:34:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:34:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:35:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:35:04	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:35:04	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:35:04	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:35:04	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:35:04	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 19:35:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 19:35:09	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:35:09	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 19:35:09	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 19:35:09	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0

			19:35:09		
Security	Audit Success	13824	2020-09-12 19:35:22	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	12290	2020-09-12 19:35:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:35:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 19:35:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 19:40:13	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:41:23	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI

	Success		12 19:44:44	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 19:44:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:44:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:44:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:44:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:44:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:49:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:49:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 19:52:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:52:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:54:47	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 19:54:53	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 19:54:53	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 19:54:53	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:48	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			19:59:48		
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:49	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 19:59:50	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:00:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:00:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		12 20:00:00	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 20:00:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:00:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:00:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:00:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:04:51	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 20:07:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:07:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12544	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:09:52	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	12544	2020-09-12 20:10:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S [illegible] ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I [illegible] x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:10:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13826	2020-09-12 20:10:32	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 20:10:32	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-12 20:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:11:23	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:14:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:14:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:14:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:14:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:14:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:14:54	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:19:55	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 20:20:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:20:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:20:21	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 20:20:22	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 20:20:22	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 20:20:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12544	2020-09-12 20:20:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:20:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID [illegible]06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:25	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 20:22:32	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x3530 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x3530 Process Name: C:\Windows\ the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most common network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cas intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Process ID: 0x3530 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is gener
Security	Audit Success	12544	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x3530 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12544	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x3530 Process Name: C:\W generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in s intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protoc
Security	Audit Success	12548	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	12548	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-0-2 Account Name: DWM-2 Account Domain: Window Manage
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:22:33		

Navigation

Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:22:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12545	2020-09-12 20:22:44	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Doma
Security	Audit Success	12545	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-96-0-1 Account Name: UMFD-1 Account Domain: Font Driver Host Logon ID: 0
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:22:45	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12545	2020-09-12 20:22:48	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	12545	2020-09-12 20:22:48	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0
Security	Audit Success	13824	2020-09-12 20:48:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF

Security	Audit Success	13824	2020-09-12 20:48:10	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Se Navigation ıt Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12544	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x594 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xeb86e7 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon ID: 0xeb8690 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13826	2020-09-12 20:48:12	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	12290	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: Operation Information: File Path: C:\Users\bebos\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_970e8aca
Security	Audit Success	12292	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Additional Information: Operation: %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:13	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit	13824	2020-09-	Microsoft-Windows-	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x

	Success		12 20:48:13	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 20:48:14	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723

			20:48:18		

Navigation

Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-23344[illegible]-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b0e870aa6
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\b0e870aa6
Security	Audit Success	12292	2020-09-12 20:48:18	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 20:48:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:19	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:20	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12292	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0
Security	Audit Success	12292	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0 0x0

Security	Audit Success	12544	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Secu Navigation Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x594 Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 127.0.0.1 Port: 0
Security	Audit Success	12544	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0xf14791 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0xf14712 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originate correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Pack
Security	Audit Success	12544	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORK Information: Process ID: 0x2e4 Process Name: C:\Windows\System32\lsass.exe Network Information: Network Address: - Port: - This event
Security	Audit Success	12544	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0xf16ad5 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12544	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon ID: 0xf16a3c Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Proce event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the accoun new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name ind
Security	Audit Success	12545	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12545	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account
Security	Audit Success	12548	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	12548	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: b
Security	Audit Success	13824	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 20:48:22	Microsoft-Windows-Security-Auditing	4738: A user account was changed. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0 Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: - New UAC Value: - User Account Control: - User Parameters: - SID His
Security	Audit Success	13824	2020-09-12 20:48:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 20:48:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12 20:48:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOR

			20:48:25		
Security	Audit Success	13824	2020-09-12 20:48:25	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	12290	2020-09-12 20:48:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 20:48:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 20:48:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 20:48:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:26	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WOF
Security	Audit Success	13824	2020-09-12 20:48:29	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x
Security	Audit Success	13824	2020-09-12 20:48:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:44	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

Navigation

	Success		12 20:48:45	Security-Auditing	
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:48:45		

Navigation

Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:45	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

	Success		12 20:48:46	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:46	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP L Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s

			20:48:56		that was accessed. The subject fields indicate the account on the local ... the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name i Navigation may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:48:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	13824	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:58	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12290	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.549981c3f5f10_8wekyb3d8bbwe\AC\Microsoft\Crypto\TokenBindingKeys\Keys\c65525a9c
Security	Audit Success	12292	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 20:48:59	Security-Auditing	
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:48:59		

Navigation

Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:48:59	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Failure	12290	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-23344 Navigation	96394-1001 Account Name: bebos Account D
Security	Audit Failure	12290	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12290	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D	
Security	Audit Success	12292	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0	
Security	Audit Success	12292	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723	
Security	Audit Success	12292	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5382: Vault credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Logon ID: 0x	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:00	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		12 20:49:01	Security-Auditing	Navigation
Security	Audit Success	13824	2020-09-12 20:49:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:01	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 20:49:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 20:49:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 20:49:24	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 20:49:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:29	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 20:49:30	Security-Auditing	
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:49:30		

Navigation

Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:30	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:31	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:32	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Navigation

	Success		12 20:49:33	Security-Auditing	
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:33	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:49:35		
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID	Navigation 06551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:35	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:36	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	
Security	Audit	13824	2020-09-	Microsoft-Windows-	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:	

	Success		12 20:49:37	Security-Auditing	
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			20:49:37		

Navigation

Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 20:49:37	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12544	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12548	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUI
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:

			21:03:15		
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	13824	2020-09-12 21:03:15	Microsoft-Windows-Security-Auditing	5379: Credential Manager credentials were read. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name:
Security	Audit Success	12544	2020-09-12 21:03:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 21:03:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

Navigation

	Success		12 21:03:57	Security-Auditing	
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

			21:03:57		
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10
Security	Audit Success	13826	2020-09-12 21:03:57	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-10

Security	Audit Success	12544	2020-09-12 21:04:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process I ‹2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 21:04:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

			21:04:27		
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S Navigation -21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:04:27	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	12290	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit	12290	2020-09-	Microsoft-Windows-	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D

	Success		12 21:05:24	Security-Auditing	Navigation
Security	Audit Success	12292	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 21:05:24	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 21:05:26	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 21:05:26	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 21:05:26	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 21:07:37	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 21:07:37	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 21:07:37	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	12290	2020-09-12 21:11:15	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 21:11:15	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 21:11:15	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12290	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12290	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0
Security	Audit Success	12292	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\cf5cb1723
Security	Audit Success	12292	2020-09-12	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D %%2464 Return Code: 0x0

			21:11:16		
Security	Audit Success	12544	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S Navigation ETHOANG$ Account Domain: WORKGROUP Lo Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\s that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service su indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impers have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indica
Security	Audit Success	12548	2020-09-12 21:11:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Log
Security	Audit Success	12290	2020-09-12 21:11:17	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D
Security	Audit Success	12292	2020-09-12 21:11:17	Microsoft-Windows-Security-Auditing	5058: Key file operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account Domain: C:\Users\bebos\AppData\Local\Packages\microsoft.windows.search_cw5n1h2txyewy\AC\Microsoft\Crypto\TokenBindingKeys\Keys\887a471fc
Security	Audit Success	12292	2020-09-12 21:11:17	Microsoft-Windows-Security-Auditing	5059: Key migration operation. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Account Name: bebos Account D Return Code: 0x0
Security	Audit Success	13826	2020-09-12 21:11:21	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13826	2020-09-12 21:11:21	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-18 Account Name: VIETHOANG$ Account Do
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit	13824	2020-09-	Microsoft-Windows-	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

	Success		12 21:11:42	Security-Auditing	

Navigation

Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun

			21:11:42		
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13824	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4798: A user's local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1001 Accoun
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42	Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(

Security	Audit Success	13826	2020-09-12 21:11:42		Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. S Navigation -21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42		Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
Security	Audit Success	13826	2020-09-12 21:11:42		Microsoft-Windows-Security-Auditing	4799: A security-enabled local group membership was enumerated. Subject: Security ID: S-1-5-21-233448718-3606551117-1202096394-1(
System	Warning	None	2020-09-08 01:44:34	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 01:46:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-08 11:54:25		Service Control Manager	7023: The netprofm service terminated with the following error: %%21
System	Warning	1014	2020-09-08 11:55:01	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Error	None	2020-09-08 11:56:25		Service Control Manager	7023: The Network List Service service terminated with the following error: %%21
System	Error	None	2020-09-08 11:56:25	SYSTEM	DCOM	10010: The server {A47979D2-C419-11D9-A5B4-001185AD2B89} did not register with DCOM within the required timeout.
System	Error	None	2020-09-08 11:56:27		Service Control Manager	7030: The Printer Extensions and Notifications service is marked as an interactive service. However, the system is configured to not allow inte
System	Warning	1014	2020-09-08 11:58:17	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-08 12:02:00	LOCAL SERVICE	Microsoft-Windows-Time-Service	134: NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on 'time.windows.com,0x9'. NtpClier
System	Warning	None	2020-09-08 12:02:26	LOCAL SERVICE	Microsoft-Windows-Time-Service	134: NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on 'time.windows.com,0x9'. NtpClier
System	Warning	1014	2020-09-08 12:02:38	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-08 12:03:33	LOCAL SERVICE	Microsoft-Windows-Time-Service	134: NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on 'time.windows.com,0x9'. NtpClier
System	Warning	None	2020-09-08 14:05:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:05:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:24:00	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:24:07	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:24:15	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:24:23	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A

			08 14:24:51			Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neu Navigation (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:25:12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:25:39	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:25:46	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:25:56	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:26:12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:26:23	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:27:13	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:27:44	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:27:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:28:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:28:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:28:47	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:29:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:29:31	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:29:59	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:30:06	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:30:27	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:30:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:31:00	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:31:08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

			14:32:22			
System	Warning	None	2020-09-08 14:32:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:32:39	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:33:04	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:33:12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:33:27	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:33:43	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:34:07	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:34:14	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:34:23	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:34:32	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:34:51	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:34:59	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:35:06	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:35:13	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:35:21	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:35:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:35:36	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:35:49	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:36:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:36:49	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:37:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

	System	Warning	None	2020-09-08 14:37:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Ac Navigation COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:37:37	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:37:51	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:38:15	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:38:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:39:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:42:49	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:42:57	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
	System	Error	None	2020-09-08 14:53:04		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
	System	Error	None	2020-09-08 14:53:19		Service Control Manager	7043: The CSR OBEX Service service did not shut down properly after receiving a preshutdown control.
	System	Warning	212	2020-09-08 14:53:35	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
	System	Warning	1014	2020-09-08 14:53:45	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	1014	2020-09-08 14:53:48	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	None	2020-09-08 14:54:14	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
	System	Warning	None	2020-09-08 14:54:17	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
	System	Warning	None	2020-09-08 14:54:50	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
	System	Warning	None	2020-09-08 14:54:56	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-08 14:55:43	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-08 14:55:43	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-08 14:55:43	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-08 14:55:43	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows

			08 14:55:43			
System	Warning	None	2020-09-08 14:55:47	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-08 14:55:55	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:56:02	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:56:13	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:58:16	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:59:21	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 14:59:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 15:00:08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 15:00:26	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 15:04:28	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	1014	2020-09-08 17:15:07	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-08 17:15:25	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-08 17:16:16	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	1014	2020-09-08 19:16:59	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-08 20:03:59	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:36:56	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-08 20:42:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-08 20:45:52		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
System	Warning	212	2020-09-08 20:46:11	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
System	Warning	1014	2020-09-08 20:46:21	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-08	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.

			20:46:23			
System	Warning	None	2020-09-08 20:46:42	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-08 20:46:43	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-08 20:46:52	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-08 20:47:05	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:42	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:42	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:47:43	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:48:23	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-08 20:48:23	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-08 20:48:23	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-08 20:48:59	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:49:00	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:49:00	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-08 20:49:01	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

	System	Warning	None	2020-09-08 20:49:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Ac Navigation COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:20:48	LOCAL SERVICE	Microsoft-Windows-Time-Service	134: NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on 'time.windows.com,0x9'. NtpClier
	System	Warning	1014	2020-09-09 01:20:57	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	None	2020-09-09 01:25:24	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 using the Component Services administrative tool.
	System	Warning	None	2020-09-09 01:28:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:28:22	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:29:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:29:26	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 using the Component Services administrative tool.
	System	Warning	None	2020-09-09 01:29:36	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:33:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Error	1	2020-09-09 01:35:39	SYSTEM	Microsoft-Windows-WindowsUpdateClient	20: Installation Failure: Windows failed to install the following update with error 0x80240017: Update for Windows Defender Antivirus antima
	System	Warning	None	2020-09-09 01:44:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:46:14	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:46:21	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:46:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:46:42	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 01:47:23	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-09 02:15:18	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Error	None	2020-09-09 02:18:22	SYSTEM	DCOM	10005: DCOM got error "1115" attempting to start the service CsrBtService with arguments "Unavailable" in order to run the server: {BFF684
	System	Warning	1014	2020-09-09 02:18:53	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	None	2020-09-09 02:19:21	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
	System	Warning	None	2020-	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows

			09 02:19:21			tool.
System	Warning	None	2020-09-09 02:20:47	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 02:20:47	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 02:20:47	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 02:21:02	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 02:46:06	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-09 02:46:16	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-09 03:27:12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:27:14	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:29:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:29:04	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:33:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:33:46	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:33:49	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:38:10	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:38:42	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:39:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 03:42:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-09 17:51:10	SYSTEM	Microsoft-Windows-Kernel-Boot	29: The system cannot write to the specified device.
System	Error	None	2020-09-09 17:51:16		EventLog	6008: The previous system shutdown at 8:46:13 PM on ?9/?8/?2020 was unexpected.
System	Warning	1014	2020-09-09 17:51:24	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-09	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.

			17:51:37			
System	Error	None	2020-09-09 17:51:45		BugCheck	1001: The computer has rebooted from a bugcheck. The bugcheck was: 0x0000009f (0x0000000000000003, 0xffffb70a6ac85980, 0xfffff800
System	Warning	None	2020-09-09 17:51:51	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-09 17:51:53	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-09 17:53:26	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 17:53:26	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 17:53:26	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	1014	2020-09-09 19:41:38	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-09 19:41:40	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-09 19:41:59	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-09 19:48:45	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 19:48:47	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 19:48:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-09 20:00:20		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
System	Warning	212	2020-09-09 20:00:40	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
System	Warning	1014	2020-09-09 20:00:52	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-09 20:00:54	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-09 20:01:32	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-09 20:01:32	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-09 20:02:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:02:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:02:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

System	Warning	None	2020-09-09 20:02:50	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Navigation e COM Server application with CLSID Windows
System	Warning	None	2020-09-09 20:02:50	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 20:02:50	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-09 20:03:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:05:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:06:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:06:05	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:06:18	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:06:20	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {259 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-09 20:07:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:22	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:07:54	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:10:55	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:11:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:11:10	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A

			09 20:12:14			Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neu Navigation (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:12:21	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:12:23	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:12:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:18:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:28:11	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:34:08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 20:42:44	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:08:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:09:24	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:22:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:22:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:22:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:24:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:24:37	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:24:39	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:24:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:24:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:24:54	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:33:50	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09 21:35:45	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

			21:35:52			
System	Warning	1014	2020-09-10 15:57:06	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-10 15:57:26	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-10 16:04:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:04:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:04:52	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:04:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:04:57	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:05:08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:05:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:05:10	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:05:25	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:06:15	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:06:17	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:06:18	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:06:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:07:39	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:07:46	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:39:50	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:39:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:42:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 16:42:54	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

	System	Warning	None	2020-09-10 16:43:13	bebos	DCOM	10016: The machine-default permission settings do not grant Local Ac Navigation COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:43:16	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:43:21	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:44:16	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Error	None	2020-09-10 16:54:15	SYSTEM	Schannel	36871: A fatal error occurred while creating a TLS client credential. The internal error state is 10013.
	System	Warning	None	2020-09-10 16:54:22	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:55:58	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:56:07	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:56:26	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:56:45	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 16:58:08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Error	None	2020-09-10 16:59:25	SYSTEM	Schannel	36871: A fatal error occurred while creating a TLS client credential. The internal error state is 10013.
	System	Warning	None	2020-09-10 17:07:32	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-10 17:07:38	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
	System	Warning	1014	2020-09-10 18:19:56	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	None	2020-09-10 18:20:04	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
	System	Error	None	2020-09-10 18:20:07	bebos	DCOM	10001: Unable to start a DCOM Server: Microsoft.Windows.ContentDeliveryManager_10.0.19041.423_neutral_neutral_cw5n1h2txyewy!App.A
	System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
	System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
	System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
	System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
	System	Error	None	2020-09-	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.

Navigation

			10 18:20:22			
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:22	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.

			18:20:23			
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:23	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.

System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} di(Navigation vithin the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:24	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.

			10 18:20:25			Navigation
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:25	bebos	DCOM	10010: The server {D63B10C5-BB46-4990-A94F-E40B9D520160} did not register with DCOM within the required timeout.
System	Error	None	2020-09-10 18:20:43		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
System	Warning	1014	2020-09-10 18:21:11	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-10 18:21:13	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-10 18:21:34	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-10 18:21:35	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-10	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows

			18:23:12			
						Navigation
System	Warning	None	2020-09-10 18:23:12	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-10 18:23:12	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	1014	2020-09-10 18:52:54	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-10 18:58:39	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-10 19:00:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:00:54	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:12:00	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:16:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-10 19:20:26		EventLog	6008: The previous system shutdown at 6:21:03 PM on ?9/?10/?2020 was unexpected.
System	Warning	1014	2020-09-10 19:20:34	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-10 19:20:36	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Error	None	2020-09-10 19:20:37		BugCheck	1001: The computer has rebooted from a bugcheck. The bugcheck was: 0x0000007f (0x0000000000000008, 0xffffa8009ea46e50, 0xffffc181
System	Warning	None	2020-09-10 19:21:08	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-10 19:21:08	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-10 19:21:14	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:21:16	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:21:17	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:21:49	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:22:02	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:22:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:22:06	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

System	Warning	None	2020-09-10 19:22:34	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Navigation e COM Server application with CLSID Windows
System	Warning	None	2020-09-10 19:22:34	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-10 19:22:34	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-10 19:24:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-10 19:24:56	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	1014	2020-09-11 11:21:55	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-11 11:22:10	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-11 11:28:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 11:28:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 11:28:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 11:36:08	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-11 11:39:37		EventLog	6008: The previous system shutdown at 8:40:26 PM on ?9/?10/?2020 was unexpected.
System	Warning	1014	2020-09-11 11:39:45	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Error	None	2020-09-11 11:39:46		BugCheck	1001: The computer has rebooted from a bugcheck. The bugcheck was: 0x0000007f (0x0000000000000008, 0xffffa80056446e50, 0xfffff50b
System	Warning	None	2020-09-11 11:41:45	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-11 12:17:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:17:47	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-11 12:17:51	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-11 12:18:42	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:18:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:18:54	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A

			11 12:19:02			Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neu Navigation (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:19:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:19:12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:19:15	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:19:16	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:21:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:23:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:24:22	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:24:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:24:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:24:34	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:25:06	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:25:22	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:25:25	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:25:25	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:25:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:35:12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:35:52	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:57:00	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 12:59:02	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:01:31	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

			13:13:27			
System	Warning	None	2020-09-11 13:13:44	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:20:58	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:21:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:21:16	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:21:28	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:24:48	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-11 13:27:15	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-11 13:29:31	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:32:02	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:32:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:32:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:48:14	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 13:54:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	1014	2020-09-11 18:12:18	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-11 18:12:22	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-11 18:12:35	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-11 18:12:46	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-11 18:14:18	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-11 18:26:51	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 18:26:54	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-11 18:26:58	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

	System	Warning	None	2020-09-11 18:27:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Ac Navigation COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 19:00:13	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 19:49:10	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
	System	Warning	None	2020-09-11 19:52:16	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
	System	Error	None	2020-09-11 19:54:13	SYSTEM	DCOM	10005: DCOM got error "1115" attempting to start the service CsrBtService with arguments "Unavailable" in order to run the server: {BFF68
	System	Warning	212	2020-09-11 19:54:32	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
	System	Warning	1014	2020-09-11 19:54:42	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	1014	2020-09-11 19:54:45	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
	System	Warning	None	2020-09-11 19:55:09	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
	System	Warning	None	2020-09-11 19:55:09	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
	System	Warning	None	2020-09-11 19:55:13	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 19:55:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 19:55:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 19:55:41	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 19:56:48	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-11 19:56:48	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-11 19:56:48	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
	System	Warning	None	2020-09-11 19:57:11	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
	System	Warning	None	2020-09-11 19:57:30	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
	System	Warning	None	2020-09-11 19:57:40	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
	System	Warning	None	2020-09-11 20:21:21	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
	System	Warning	None	2020-09-	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A

			11 20:55:20			Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neu Navigation (S-1-15-2-155514346-2573954481-7557412
System	Warning	1014	2020-09-12 11:20:57	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 11:21:13	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 11:21:14	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 11:23:57	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 11:24:36	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:24:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:24:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:24:45	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:24:51	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:24:53	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:24:56	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:25:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:25:32	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-12 11:25:56	SYSTEM	DCOM	10005: DCOM got error "1115" attempting to start the service CsrBtService with arguments "Unavailable" in order to run the server: {BFF68
System	Warning	212	2020-09-12 11:26:15	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
System	Warning	1014	2020-09-12 11:26:27	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 11:26:29	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 11:26:52	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-12 11:26:53	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 11:27:47	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

			11:27:49			
System	Warning	None	2020-09-12 11:27:50	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:27:55	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 11:28:30	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 11:28:30	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 11:28:30	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 11:39:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	1014	2020-09-12 11:49:51	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name _ldap._tcp.dc._msdcs.WORKGROUP timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 11:50:32	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:50:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:50:35	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 11:50:36	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-12 11:50:43	bebos	DCOM	10010: The server {9BA05972-F6A8-11CF-A442-00A0C90A8F39} did not register with DCOM within the required timeout.
System	Error	None	2020-09-12 11:50:59		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
System	Error	None	2020-09-12 11:51:15		Service Control Manager	7043: The CSR Bluetooth Service service did not shut down properly after receiving a preshutdown control.
System	Warning	212	2020-09-12 11:51:34	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
System	Warning	1014	2020-09-12 11:51:44	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 11:51:46	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 11:52:05	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 11:52:07	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-12 11:53:46	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 11:53:46	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows

System	Warning	None	2020-09-12 11:53:46	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Navigation COM Server application with CLSID Windows
System	Warning	None	2020-09-12 11:55:37	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 11:56:01	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 12:05:39	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 12:05:42	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 12:58:47	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 12:58:47	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 13:08:56	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	1014	2020-09-12 15:42:11	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 15:42:23	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 15:42:40	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 15:42:49	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 15:43:51	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 15:44:00	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 15:55:28	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 15:55:29	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 15:55:30	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 15:55:31	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 15:55:32	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 15:55:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 15:55:39	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A

			12 16:01:43			Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neu Navigation (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:09:50	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:10:10	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-12 16:15:10		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
System	Warning	212	2020-09-12 16:15:27	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
System	Warning	1014	2020-09-12 16:15:36	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 16:15:39	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 16:16:00	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-12 16:16:00	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 16:16:12	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 16:16:22	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:16:52	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:17:38	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:17:39	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 16:17:39	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 16:17:39	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 16:18:20	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:19:59	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:24:48	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:25:07	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:25:25	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

			16:26:03			
System	Warning	None	2020-09-12 16:26:23	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:26:33	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:26:45	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 16:27:01	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 17:15:34	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 17:15:55	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	1014	2020-09-12 18:46:14	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 18:46:21	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 19:06:17	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Error	None	2020-09-12 19:07:00		Service Control Manager	7043: The CSR Bluetooth Audio Service service did not shut down properly after receiving a preshutdown control.
System	Error	None	2020-09-12 19:07:15		Service Control Manager	7043: The CSR Bluetooth Service service did not shut down properly after receiving a preshutdown control.
System	Warning	212	2020-09-12 19:07:33	SYSTEM	Microsoft-Windows-Kernel-PnP	219: The driver \Driver\WudfRd failed to load for the device USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\7&2f89c034&0&(
System	Warning	1014	2020-09-12 19:07:43	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 19:07:45	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 19:08:07	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 19:08:07	bebos	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows tool.
System	Warning	None	2020-09-12 19:08:21	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 19:09:19	LOCAL SERVICE	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {6B3E administrative tool.
System	Warning	None	2020-09-12 19:09:19	LOCAL SERVICE	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A administrative tool.
System	Warning	None	2020-09-12 19:09:19	LOCAL SERVICE	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {6B3E administrative tool.
System	Warning	None	2020-09-12 19:09:19	LOCAL SERVICE	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A administrative tool.

System	Warning	None	2020-09-12 19:09:42	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Navigation e COM Server application with CLSID Windows
System	Warning	None	2020-09-12 19:09:42	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 19:09:42	SYSTEM	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows
System	Warning	None	2020-09-12 19:40:14	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 19:40:14	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 19:49:40	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 20:00:01	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	1014	2020-09-12 20:22:36	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 20:48:13	LOCAL SERVICE	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {6B3E administrative tool.
System	Warning	None	2020-09-12 20:48:13	LOCAL SERVICE	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {6B3E administrative tool.
System	Warning	1014	2020-09-12 20:48:14	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name _VLMCS._TCP timed out after none of the configured DNS servers responded.
System	Warning	1014	2020-09-12 20:48:21	NETWORK SERVICE	Microsoft-Windows-DNS-Client	1014: Name resolution for the name wpad timed out after none of the configured DNS servers responded.
System	Warning	None	2020-09-12 20:48:32	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 This security permission can be modified using the Component Services administrative tool.
System	Warning	None	2020-09-12 20:48:44	bebos	DCOM	10016: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593 Component Services administrative tool.
System	Warning	None	2020-09-12 21:03:09	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412
System	Warning	None	2020-09-12 21:05:03	bebos	DCOM	10016: The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-7557412

Database Software

Database Drivers:

Borland Database Engine	-
Borland InterBase Client	-
Easysoft ODBC-InterBase 6	-
Easysoft ODBC-InterBase 7	-
Firebird Client	-
Jet Engine	4.00.9801.27
MDAC	10.0.19041.329 (WinBuild.160101.0800)

ODBC	10.0.19041.1 (WinBuild.160101.0800)
MySQL Connector/ODBC	-
Oracle Client	-
PsqlODBC	-
Sybase ASE ODBC	-

Database Servers:

Borland InterBase Server	-
Firebird Server	-
Microsoft SQL Server	-
Microsoft SQL Server Compact Edition	-
Microsoft SQL Server Express Edition	-
MySQL Server	-
Oracle Server	-
PostgreSQL Server	-
Sybase SQL Server	-

Navigation

ODBC Drivers

Driver Description	File Name	Version	File Extensions Supported
Driver da Microsoft para arquivos texto (*.txt; *.csv)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.,*.asc,*.csv,*.tab,*.txt,*.csv
Driver do Microsoft Access (*.mdb)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.mdb
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
Driver do Microsoft Excel(*.xls)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.xls
Driver do Microsoft Paradox (*.db)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.db
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
Microsoft Access-Treiber (*.mdb)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.mdb
Microsoft dBase Driver (*.dbf)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.dbf,*.ndx,*.mdx
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
Microsoft Excel Driver (*.xls)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.xls
Microsoft Excel-Treiber (*.xls)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.xls
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
Microsoft Paradox Driver (*.db)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.db
Microsoft Paradox-Treiber (*.db)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.db
[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]	[TRIAL VERSION]
Microsoft Text-Treiber (*.txt; *.csv)	odbcjt32.dll	10.0.19041.1 (WinBuild.160101.0800)	*.,*.asc,*.csv,*.tab,*.txt,*.csv
SQL Server	sqlsrv32.dll	10.0.19041.1 (WinBuild.160101.0800)	

ODBC Data Sources

Data Source Name	Data Source Description	Type	Driver File Name
dBASE Files	Microsoft Access dBASE Driver (*.dbf, *.ndx, *.mdx)	User	aceodbc.dll
Excel Files	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.xlsb)	User	aceodbc.dll
MS Access Database	Microsoft Access Driver (*.mdb, *.accdb)	User	aceodbc.dll

Memory Read

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS

111245 MB/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	
85715 MB/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	18-18-18-38 CR1
77068 MB/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
68474 MB/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
68050 MB/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
59309 MB/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
54885 MB/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
52263 MB/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
47090 MB/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
45280 MB/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
45200 MB/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
44459 MB/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
42764 MB/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
41312 MB/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
39542 MB/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
38265 MB/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
35611 MB/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
31589 MB/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
30690 MB/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
27404 MB/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
27235 MB/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
26279 MB/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
24854 MB/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
23639 MB/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
23246 MB/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
21557 MB/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
21290 MB/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
21240 MB/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
21238 MB/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
21178 MB/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
21007 MB/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
20056 MB/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
19189 MB/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
18848 MB/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
17754 MB/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
16602 MB/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
16436 MB/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
15717 MB/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
14716 MB/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
14070 MB/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
13509 MB/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
13158 MB/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
11433 MB/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
11314 MB/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
11214 MB/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
10581 MB/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
10204 MB/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
9660 MB/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1

9021 MB/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	
8734 MB/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	
8543 MB/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
8160 MB/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
7992 MB/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
7620 MB/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
7540 MB/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
6560 MB/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
6431 MB/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
6238 MB/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
6013 MB/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
6000 MB/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
5833 MB/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
5392 MB/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
5334 MB/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
4591 MB/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
3971 MB/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
3938 MB/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
3672 MB/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
3569 MB/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
3364 MB/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
3323 MB/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
2919 MB/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2

Navigation

Memory Write

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
93960 MB/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
87145 MB/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
73605 MB/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
73328 MB/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
65654 MB/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
60036 MB/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
57968 MB/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
53174 MB/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
53051 MB/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
46700 MB/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
45695 MB/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
44521 MB/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
43931 MB/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
40821 MB/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
40019 MB/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
33260 MB/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
33252 MB/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
32976 MB/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
27387 MB/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
23902 MB/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2

Navigation

23664 MB/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	
23651 MB/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
19577 MB/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
17670 MB/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
17365 MB/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
17092 MB/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
16992 MB/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
16893 MB/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
16676 MB/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
14837 MB/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
14246 MB/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
13065 MB/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
12775 MB/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
12475 MB/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
11929 MB/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
11630 MB/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
10653 MB/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
10227 MB/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
10159 MB/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
9953 MB/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
9949 MB/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
9814 MB/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
9323 MB/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
8864 MB/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
8646 MB/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
7921 MB/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
7706 MB/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
7114 MB/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
7091 MB/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
7083 MB/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
6734 MB/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
5654 MB/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
5638 MB/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
5518 MB/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
4868 MB/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
4829 MB/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
4696 MB/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
4592 MB/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
4260 MB/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
4219 MB/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
4094 MB/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
4074 MB/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
3803 MB/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
3652 MB/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
3561 MB/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
3154 MB/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
2831 MB/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

2797 MB/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	
2472 MB/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	
2335 MB/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
2327 MB/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12

Navigation

Memory Copy

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
103987 MB/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
95761 MB/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
67171 MB/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
67051 MB/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
66492 MB/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
55043 MB/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
54396 MB/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
51658 MB/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
50972 MB/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
47965 MB/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
42705 MB/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
40993 MB/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
40461 MB/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
38295 MB/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
37901 MB/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
34718 MB/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
31262 MB/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
30678 MB/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
26791 MB/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
24893 MB/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
24569 MB/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
24464 MB/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
24331 MB/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
23704 MB/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
22688 MB/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
22048 MB/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
21684 MB/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
19590 MB/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
17604 MB/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
17551 MB/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
17365 MB/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
17343 MB/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
17256 MB/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
16691 MB/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
15854 MB/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
15829 MB/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
15257 MB/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
14927 MB/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
14078 MB/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1

14015 MB/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	
12460 MB/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
12113 MB/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
11321 MB/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
11246 MB/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
9930 MB/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
9653 MB/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
9482 MB/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
8936 MB/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
8217 MB/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
7656 MB/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
7609 MB/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
7389 MB/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
6278 MB/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
6127 MB/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
5911 MB/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
5510 MB/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
5287 MB/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
4893 MB/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
4777 MB/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
4690 MB/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
4551 MB/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
4237 MB/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
4194 MB/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
4174 MB/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
3681 MB/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
3269 MB/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
3145 MB/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
3051 MB/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
3000 MB/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
2987 MB/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
2576 MB/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2

Navigation

Memory Latency

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
55.2 ns	Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
57.1 ns	Core i7-3770K	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
58.3 ns	Core i7-4770	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
59.5 ns	Core i7-8700K	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
59.9 ns	A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
60.1 ns	Core i7-7700K	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
60.5 ns	Core i7-6700K	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
60.9 ns	FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
61.0 ns	Core i7-4930K	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
61.2 ns	FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2

62.5 ns	FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	
62.9 ns	A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
63.1 ns	Core i7-965 Extreme	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
66.4 ns	Core i7-2600	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
66.8 ns	Core i7-990X Extreme	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
67.3 ns	Core i7-5775C	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
67.5 ns	Core i7-3960X Extreme	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
67.9 ns	Ryzen 9 3950X	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
69.6 ns	Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
70.4 ns	Xeon X5550	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
70.5 ns	Core i7-6850K	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
71.2 ns	Ryzen Threadripper 2990WX	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
72.0 ns	Core i7-5820K	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
72.5 ns	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
73.1 ns	Ryzen 7 2700X	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
73.8 ns	Ryzen 5 2400G	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
74.0 ns	Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
74.2 ns	Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
76.0 ns	A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
76.8 ns	**Core i3-3220**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
77.0 ns	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
77.1 ns	Core i7-7800X	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
78.5 ns	Pentium EE 955	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
79.5 ns	Xeon E5-2670	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
79.8 ns	Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
81.4 ns	Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
82.4 ns	A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
82.4 ns	Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
82.5 ns	Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
82.6 ns	P4EE	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
83.5 ns	Ryzen 7 1800X	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
84.6 ns	Xeon E5-2660 v3	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
85.8 ns	Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
86.7 ns	Ryzen Threadripper 3970X	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
88.1 ns	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
90.0 ns	Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
91.3 ns	Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
93.1 ns	Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
94.7 ns	Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
95.3 ns	Atom D525	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
96.9 ns	A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
99.5 ns	Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
100.4 ns	Core i5-650	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
101.2 ns	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
101.6 ns	Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
104.1 ns	Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
106.5 ns	Atom 230	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
108.3 ns	E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1

112.5 ns	Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	
113.4 ns	Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	
114.5 ns	Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
119.9 ns	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
123.5 ns	Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
123.9 ns	Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
124.7 ns	Xeon	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
127.7 ns	Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
128.2 ns	Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
129.0 ns	Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
138.7 ns	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
153.6 ns	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
159.8 ns	Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1

Navigation

CPU Queen

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
276199	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
216826	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
149985	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
146744	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
99682	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
93183	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
85483	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
72443	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
67341	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
64839	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
62693	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
62382	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
59950	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
56864	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
55275	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
54386	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
53521	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
48880	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
47712	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
47204	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
46792	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
45875	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
43962	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
42538	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
42193	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
41733	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
37779	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
36105	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
34010	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
32362	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2

31729	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	
30788	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
26992	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
25503	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
22146	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
22010	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
21993	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
21796	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
21669	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
21669	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
21454	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
21431	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
21226	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
20130	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
19490	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
19484	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
19232	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
18844	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
18011	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
16868	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
16100	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
15584	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
14761	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
12584	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
12147	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
11234	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
8547	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
7464	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
7287	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
5916	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
5444	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
5165	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
4078	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
4025	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
3855	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
3791	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
3514	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
3301	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
2815	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
2586	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
1839	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2

Navigation

CPU PhotoWorxx

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
61896 MPixel/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1

56098 MPixel/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	
38828 MPixel/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	
38788 MPixel/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
38361 MPixel/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
35548 MPixel/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
30449 MPixel/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
26642 MPixel/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
24221 MPixel/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
23753 MPixel/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
23510 MPixel/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
23412 MPixel/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
22800 MPixel/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
20497 MPixel/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
20422 MPixel/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
19743 MPixel/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
19369 MPixel/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
19250 MPixel/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
17044 MPixel/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
15634 MPixel/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
14159 MPixel/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
14009 MPixel/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
12969 MPixel/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
12359 MPixel/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
12350 MPixel/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
11904 MPixel/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
11889 MPixel/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
11589 MPixel/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
11089 MPixel/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
10676 MPixel/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
9568 MPixel/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
9091 MPixel/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
8902 MPixel/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
8800 MPixel/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
8593 MPixel/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
8546 MPixel/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
8073 MPixel/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
7926 MPixel/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
7765 MPixel/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
6976 MPixel/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
6876 MPixel/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
6210 MPixel/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
6111 MPixel/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
5627 MPixel/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
5276 MPixel/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
4792 MPixel/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
4726 MPixel/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
4243 MPixel/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
4214 MPixel/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2

3847 MPixel/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-80	
3701 MPixel/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	
3459 MPixel/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
3004 MPixel/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
2927 MPixel/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
2790 MPixel/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
2536 MPixel/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
2146 MPixel/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
1998 MPixel/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
1901 MPixel/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
1895 MPixel/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
1869 MPixel/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
1864 MPixel/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
1852 MPixel/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
1788 MPixel/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
1676 MPixel/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
1253 MPixel/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
1220 MPixel/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
1102 MPixel/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
1096 MPixel/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
878 MPixel/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
831 MPixel/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2

Navigation

CPU ZLib

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
3233.9 MB/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
2475.9 MB/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
1642.9 MB/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
1216.8 MB/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
977.6 MB/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
751.8 MB/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
685.5 MB/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
672.5 MB/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
575.1 MB/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
544.1 MB/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
493.8 MB/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
453.8 MB/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
437.7 MB/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
432.5 MB/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
415.0 MB/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
407.1 MB/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
365.9 MB/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
359.9 MB/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
357.7 MB/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
356.9 MB/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
347.3 MB/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1

345.2 MB/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	Navigation
326.0 MB/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
317.0 MB/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
313.7 MB/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
286.5 MB/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
281.2 MB/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
275.1 MB/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
256.3 MB/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
243.7 MB/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
224.6 MB/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
209.5 MB/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
189.0 MB/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
188.7 MB/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
186.0 MB/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
183.3 MB/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
174.9 MB/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
173.8 MB/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
169.8 MB/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
153.9 MB/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
151.9 MB/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
151.4 MB/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
140.5 MB/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
136.0 MB/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
135.1 MB/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
116.8 MB/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
112.0 MB/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
107.9 MB/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
105.3 MB/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
99.1 MB/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
97.2 MB/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
95.3 MB/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
84.0 MB/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
82.8 MB/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
73.7 MB/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
73.2 MB/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
60.0 MB/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
58.4 MB/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
41.7 MB/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
41.5 MB/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
33.3 MB/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
32.8 MB/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
32.2 MB/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
31.7 MB/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
24.0 MB/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
22.6 MB/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
19.6 MB/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
18.6 MB/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

17.4 MB/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	
16.1 MB/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	
15.3 MB/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2

Navigation

CPU AES

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
285585 MB/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
224070 MB/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
147445 MB/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
70290 MB/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
65838 MB/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
63242 MB/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
46884 MB/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
38015 MB/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
32074 MB/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
29420 MB/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
27374 MB/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
25198 MB/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
23206 MB/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
21097 MB/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
21096 MB/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
20645 MB/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
18234 MB/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
17940 MB/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
17292 MB/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
16801 MB/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
16358 MB/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
15377 MB/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
14455 MB/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
13667 MB/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
12246 MB/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
10337 MB/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
9791 MB/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
9136 MB/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
9011 MB/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
8503 MB/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
8500 MB/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
6557 MB/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
4924 MB/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
4052 MB/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
3781 MB/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
2908 MB/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
1930 MB/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
1619 MB/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
1452 MB/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
1332 MB/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2

1286 MB/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2	
1233 MB/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
1152 MB/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
914 MB/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
802 MB/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
791 MB/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
790 MB/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
721 MB/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
663 MB/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
587 MB/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
567 MB/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
524 MB/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
494 MB/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
473 MB/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
469 MB/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
421 MB/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
387 MB/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
312 MB/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
277 MB/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
269 MB/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
242 MB/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
153 MB/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
148 MB/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
144 MB/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
131 MB/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
108 MB/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
105 MB/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
99 MB/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
98 MB/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
85 MB/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
44 MB/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

CPU SHA3

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
9774 MB/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
7396 MB/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
4950 MB/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
4941 MB/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
3419 MB/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
2668 MB/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
2531 MB/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
2524 MB/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
2237 MB/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
2018 MB/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
1986 MB/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2

1804 MB/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	
1775 MB/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	
1569 MB/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
1314 MB/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
1306 MB/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
1283 MB/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
1180 MB/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
1178 MB/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
1136 MB/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
1076 MB/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
1037 MB/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
1031 MB/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
979 MB/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
912 MB/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
876 MB/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
845 MB/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
834 MB/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
796 MB/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
758 MB/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
736 MB/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
726 MB/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
684 MB/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
625 MB/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
625 MB/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
581 MB/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
577 MB/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
555 MB/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
547 MB/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
532 MB/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
525 MB/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
523 MB/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
489 MB/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
427 MB/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
418 MB/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
401 MB/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
385 MB/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
345 MB/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
329 MB/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
327 MB/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
291 MB/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
272 MB/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
269 MB/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
260 MB/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
243 MB/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
213 MB/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
205 MB/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
200 MB/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
146 MB/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2

Navigation

110 MB/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	
107 MB/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	
106 MB/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
105 MB/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
99 MB/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
96 MB/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
90 MB/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
73 MB/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
72 MB/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
65 MB/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
51 MB/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
47 MB/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

Navigation

FPU Julia

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
302606	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
149854	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
141102	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
111086	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
66364	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
62489	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
54927	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
40860	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
40283	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
38481	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
38472	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
36094	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
34017	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
30190	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
28482	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
27646	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
26893	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
24755	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
19514	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
18966	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
18453	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
18309	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
18009	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
17672	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
15941	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
15291	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
13498	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
12633	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
12205	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
11912	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
11127	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1

8958	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	
8746	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
8686	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
8531	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
8203	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
8070	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
7958	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
7598	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
7432	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
7019	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
6987	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
6526	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
6416	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
6228	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
6169	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
5655	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
5600	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
5580	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
5577	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
5235	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
4053	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
3534	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
3487	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
2443	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
2388	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
2308	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
2053	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
1988	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
1865	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
1332	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
1307	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
1112	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
958	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
911	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
892	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
794	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
701	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
640	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
589	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
513	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2

Navigation

FPU Mandel

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
160860	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
79245	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1

72961	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	
54582	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	
36624	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
32939	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
29556	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
21692	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
21329	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
20702	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
20171	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
19160	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
18312	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
15402	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
15100	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
14851	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
14256	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
12503	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
10344	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
9890	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
9781	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
9318	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
8675	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
8614	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
8068	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
7273	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
6913	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
6434	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
6212	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
6096	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
5394	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
4625	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
4515	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
4421	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
4333	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
4180	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
4040	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
3970	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
3874	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
3646	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
3454	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
3349	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
3311	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
3174	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
3149	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
3068	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
2981	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
2890	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
2840	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
2675	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1

2335	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	
1823	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	
1482	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
1449	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
1383	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
1189	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
1182	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
1062	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
1051	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
856	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
794	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
494	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
476	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
438	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
427	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
406	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
401	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
359	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
328	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
263	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
193	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

FPU SinJulia

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
55908	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
46562	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
28541	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
18481	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
16033	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
13534	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
12654	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
7786	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
7470	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
7272	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
7240	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
7218	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
7116	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
6993	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
6821	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
6511	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
6131	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
5460	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
4978	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
4826	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
4714	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
4675	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1

4658	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2	
4615	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
4586	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
4137	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
3540	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
3212	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
3100	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
2831	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
2642	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
2589	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
2304	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
2266	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
2221	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
2210	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
2156	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
2042	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
1934	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
1872	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
1855	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
1738	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
1618	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
1575	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
1480	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
1478	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
1420	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
1377	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
1260	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
1178	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
1167	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
1049	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
1021	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
974	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
959	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
945	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
942	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
810	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
516	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
503	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
463	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
452	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
359	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
327	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
284	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
277	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
262	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
261	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
205	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

202	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	
131	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	

Navigation

FP32 Ray-Trace

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
57482 KRay/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
27881 KRay/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
27293 KRay/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
18503 KRay/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
15902 KRay/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
11818 KRay/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
11356 KRay/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
8389 KRay/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
8264 KRay/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
7481 KRay/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
7408 KRay/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	16-17-17-35 CR1
7282 KRay/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
7266 KRay/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2
5988 KRay/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
5195 KRay/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
5054 KRay/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
4853 KRay/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
4789 KRay/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
3691 KRay/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
3562 KRay/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
3360 KRay/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
2868 KRay/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
2653 KRay/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
2599 KRay/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
2559 KRay/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
2556 KRay/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
2541 KRay/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
2182 KRay/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
1982 KRay/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
1911 KRay/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
1642 KRay/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
1629 KRay/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
1546 KRay/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
1513 KRay/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
1379 KRay/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
1369 KRay/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
1313 KRay/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
1252 KRay/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
1215 KRay/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
1212 KRay/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
1175 KRay/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2

1161 KRay/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-8(	Navigation
1129 KRay/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
1104 KRay/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
978 KRay/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
976 KRay/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
850 KRay/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
801 KRay/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
788 KRay/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
782 KRay/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
774 KRay/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
570 KRay/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
526 KRay/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
523 KRay/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
370 KRay/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
354 KRay/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
319 KRay/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
299 KRay/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
272 KRay/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
268 KRay/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
213 KRay/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
203 KRay/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15
165 KRay/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
145 KRay/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
130 KRay/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1
123 KRay/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
117 KRay/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
105 KRay/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
95 KRay/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12
92 KRay/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
70 KRay/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2

FP64 Ray-Trace

	CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS
31857 KRay/s	32x Ryzen Threadripper 3970X HT	3800 MHz	Gigabyte TRX40 Aorus Xtreme	TRX40	Quad DDR4-3200	16-18-18-36 CR1
15318 KRay/s	16x Ryzen 9 3950X HT	3500 MHz	Gigabyte X570 Aorus Pro WiFi	X570	Dual DDR4-3600	16-16-16-36 CR1
13887 KRay/s	32x Ryzen Threadripper 2990WX HT	3000 MHz	MSI MEG X399 Creation	X399	Quad DDR4-2933	16-18-18-38 CR1
10033 KRay/s	20x Xeon E5-2660 v3 HT	2600 MHz	Supermicro X10DRi	C612	Octal DDR4-1866	13-13-13-31 CR1
8839 KRay/s	6x Core i7-7800X HT	3500 MHz	Gigabyte X299 UD4	X299	Quad DDR4-2667	15-17-17-35 CR2
6425 KRay/s	6x Core i7-8700K HT	3700 MHz	Gigabyte Z370 Aorus Gaming 7	Z370 Int.	Dual DDR4-2667	16-18-18-38 CR2
5969 KRay/s	16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Octal DDR3-1333	9-9-9-24 CR1
4564 KRay/s	4x Core i7-7700K HT	4200 MHz	ASRock Z270 Extreme4	Z270 Ext.	Dual DDR4-2133	15-15-15-36 CR2
4187 KRay/s	8x Ryzen 7 2700X HT	3700 MHz	Asus Crosshair VII Hero	X470	Dual DDR4-2933	16-20-21-49 CR1
4132 KRay/s	6x Core i7-6850K HT	3600 MHz	Asus Strix X99 Gaming	X99	Quad DDR4-2400	16-16-16-39 CR2
4057 KRay/s	6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2
4011 KRay/s	4x Core i7-6700K HT	4000 MHz	Gigabyte GA-Z170X-UD3	Z170 Int.	Dual DDR4-2133	14-14-14-35 CR2

4000 KRay/s	8x Ryzen 7 1800X HT	3600 MHz	Asus Crosshair VI Hero	X370	Dual DDR4-2667	
3256 KRay/s	32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Octal DDR3-1600R	11-11-11-28 CR1
2807 KRay/s	6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2
2772 KRay/s	4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2
2638 KRay/s	6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2
2595 KRay/s	4x Core i7-5775C HT	3300 MHz	Gigabyte GA-Z97MX-Gaming 5	Z97 Int.	Dual DDR3-1600	11-11-11-28 CR1
1963 KRay/s	4x Ryzen 5 2400G HT	3600 MHz	ASRock A320M Pro4	A320	Dual DDR4-2933	16-15-15-35 CR1
1918 KRay/s	4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2
1817 KRay/s	4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1
1559 KRay/s	12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Quad DDR2-800R	6-6-6-18 CR1
1457 KRay/s	6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1
1388 KRay/s	8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2
1379 KRay/s	8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Hexa DDR3-1333	9-9-9-24 CR1
1367 KRay/s	16x Atom C3958	2000 MHz	Supermicro A2SDi-H-TP4F	Denverton	Dual DDR4-2400	17-17-17-39
1313 KRay/s	8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2
1159 KRay/s	8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15
1039 KRay/s	8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Quad DDR2-800R	6-6-6-18 CR1
1037 KRay/s	6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2
900 KRay/s	4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1
874 KRay/s	6x FX-6100	3300 MHz	Asus Sabertooth 990FX	AMD990FX	Dual DDR3-1866	9-10-9-27 CR2
852 KRay/s	4x A12-9800	3800 MHz	Gigabyte GA-AB350M-Gaming 3	B350 Int.	Dual DDR4-2400	14-16-16-31 CR1
826 KRay/s	**2x Core i3-3220 HT**	**3300 MHz**	**[TRIAL VERSION]**	**B75 Int.**	**DDR3-1600 SDRAM**	**11-11-11-28 CR1**
737 KRay/s	4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2
724 KRay/s	8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12
717 KRay/s	4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2
671 KRay/s	4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2
669 KRay/s	8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Quad DDR2-667R	5-5-5-15 CR1
626 KRay/s	4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2
623 KRay/s	4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1
623 KRay/s	4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1
616 KRay/s	4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2
539 KRay/s	4x Celeron J4105	1500 MHz	ASRock J4105-ITX	GeminiLakeD Int.	Dual DDR4-2400	17-17-17-39
534 KRay/s	4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15
466 KRay/s	4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15
459 KRay/s	8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1
452 KRay/s	4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2
443 KRay/s	2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1
435 KRay/s	4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2
428 KRay/s	4x Celeron J3455	1500 MHz	ASRock J3455B-ITX	ApolloLakeD Int.	Dual DDR3-1866	11-11-11-32 CR1
285 KRay/s	2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2
210 KRay/s	4x Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1
205 KRay/s	2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11
197 KRay/s	2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7
193 KRay/s	4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Quad DDR2-600R	5-5-5-15 CR1
185 KRay/s	4x Celeron N3150	1600 MHz	ASRock N3150B-ITX	Braswell Int.	Dual DDR3-1600	11-11-11-28 CR2
176 KRay/s	2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1
138 KRay/s	2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2
120 KRay/s	Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2

109 KRay/s	P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	
79 KRay/s	2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	
71 KRay/s	Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15
64 KRay/s	2x Atom D525 HT	1800 MHz	Gigabyte GA-D525TUD	NM10 Int.	DDR3-800 SDRAM	6-6-6-15 CR2
62 KRay/s	Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11 CR2
59 KRay/s	Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1
56 KRay/s	Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2
54 KRay/s	Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2
46 KRay/s	2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2
43 KRay/s	Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2
28 KRay/s	Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12

Navigation

Debug - PCI

B00 D00 F00: Intel Ivy Bridge-DT - Host Bridge/DRAM Controller

```
Offset 000:  86 80 50 01 06 00 90 20 09 00 00 06 00 00 00 00
Offset 010:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020:  00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030:  00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00 00
Offset 040:  01 90 D1 FE 00 00 00 00 01 00 D1 FE 00 00 00 00
Offset 050:  11 02 00 00 11 00 00 00 07 00 90 DF 01 00 00 DB
Offset 060:  05 00 00 F8 00 00 00 00 01 80 D1 FE 00 00 00 00
Offset 070:  00 00 00 FE 00 00 00 00 00 0C 00 FE 7F 00 00 00
Offset 080:  10 11 11 00 00 00 11 00 1A 00 00 00 00 00 00 00
Offset 090:  01 00 00 00 01 00 00 00 01 00 50 1E 01 00 00 00
Offset 0A0:  01 00 00 00 01 00 00 00 01 00 60 1E 01 00 00 00
Offset 0B0:  01 00 A0 DB 01 00 80 DB 01 00 00 DB 01 00 A0 DF
Offset 0C0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0:  09 00 0C 01 92 80 80 E2 D0 00 50 14 00 00 00 00
Offset 0F0:  00 00 00 00 00 00 00 00 C8 0F 09 00 00 00 00 00
```

B00 D02 F00: Intel Ivy Bridge-DT - Integrated Graphics Controller (DT GT1)

```
Offset 000:  86 80 52 01 07 04 90 00 09 00 00 03 00 00 00 00
Offset 010:  04 00 80 F7 00 00 00 00 0C 00 00 E0 00 00 00 00
Offset 020:  01 F0 00 00 00 00 00 00 00 00 00 00 CF 10 6D 17
Offset 030:  00 00 00 00 90 00 00 00 00 00 00 00 00 01 00 00
Offset 040:  09 00 0C 01 92 80 80 E2 D0 00 50 14 00 00 00 00
Offset 050:  11 02 00 00 11 00 00 00 00 00 00 00 01 00 A0 DB
Offset 060:  00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090:  05 D0 01 00 0C F0 E0 FE 81 49 00 00 00 00 00 00
Offset 0A0:  00 00 00 00 13 00 06 03 00 00 00 00 00 00 00 00
Offset 0B0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0:  01 A4 22 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0:  00 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00
Offset 0F0:  00 00 00 00 00 00 00 00 00 00 09 00 18 E0 B2 D9
```

B00 D14 F00: Intel Panther Point PCH - USB 3.0 xHCI Controller [C1]

Offset 000: 86 80 31 1E 06 04 90 02 04 30 03 0C 00 00 00 00
Offset 010: 04 00 C0 F7 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 70 00 00 00 00 00 00 00 00 01 00 00
Offset 040: FD 07 0E 80 39 C2 03 80 00 00 00 00 00 00 00 00
Offset 050: 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 30 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 01 80 C2 C1 08 81 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 00 87 00 0C F0 E0 FE 00 00 00 00 71 49 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 8F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 0F 00 00 00 0F 00 00 00 0F 00 00 00 0F 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D16 F00: Intel Panther Point PCH - Host Embedded Controller Interface 1 (HECI1) [C1]

Offset 000: 86 80 3A 1E 06 04 10 00 04 00 80 07 00 00 80 00
Offset 010: 04 B0 C1 F7 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 00 01 00 00
Offset 040: 45 02 00 1E 20 00 01 80 06 01 00 60 E0 0F 00 10
Offset 050: 01 8C 03 C8 08 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 05 00 81 00
Offset 090: 0C F0 E0 FE 00 00 00 00 61 49 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 C0
Offset 0C0: 92 02 5E 75 0C 42 0A 1B 46 73 6F 52 45 6D B7 E2
Offset 0D0: 6E 76 57 DE 12 DC E3 00 9C B4 FB 73 42 BB 69 64
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

B00 D1A F00: Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C1]

Offset 000: 86 80 2D 1E 06 00 90 02 04 20 03 0C 00 00 00 00
Offset 010: 00 80 C1 F7 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 10 01 00 00
Offset 040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 58 C2 C9 00 00 00 00 0A 98 A0 20 00 00 00 00
Offset 060: 20 20 81 07 00 00 00 00 01 00 00 01 00 20 00 00
Offset 070: 00 00 FF 3F 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 80 00 11 88 0C 93 30 0D 00 24 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 13 00 06 03 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 AA FF 00 00 00 00 00 00 00 00 00

Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 84 20 95 DA
Offset 0F0: 00 00 00 00 88 85 80 00 87 0F 05 08 08 17 5B 20

Navigation

B00 D1B F00: Intel Panther Point PCH - High Definition Audio Controller [C1]

Offset 000: 86 80 20 1E 06 00 10 00 04 00 03 04 10 00 00 00
Offset 010: 04 00 C1 F7 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 6C 17
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 16 01 00 00
Offset 040: 01 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 60 42 C8 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 05 70 80 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 10 00 91 00 00 00 00 10 00 08 10 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 04 02 01 00 24 00 40 00 0C A3 82 10 00 33 02
Offset 0D0: 00 0C A3 02 10 00 33 02 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1C F00: Intel Panther Point PCH - PCI Express Port 1 [C1]

Offset 000: 86 80 10 1E 04 04 10 00 C4 00 04 06 10 00 81 00
Offset 010: 00 00 00 00 00 00 00 00 00 01 01 00 F0 00 00 20
Offset 020: F0 FF 00 00 F1 FF 01 00 00 00 00 00 00 00 00 00
Offset 030: 00 00 00 00 40 00 00 00 00 00 00 00 0B 01 04 00
Offset 040: 10 80 42 01 00 80 00 00 00 00 10 00 12 4C 12 01
Offset 050: 03 00 01 10 00 B2 04 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 16 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 0D A0 00 00 CF 10 58 17 00 00 00 00 00 00 00 00
Offset 0A0: 01 00 02 C8 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 01 02 0B 00 00 00 80 11 01 00 00 00 00
Offset 0E0: 00 3F 00 00 00 00 00 00 03 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1C F01: Intel Panther Point PCH - PCI Express Port 2 [C1]

Offset 000: 86 80 12 1E 07 04 10 00 C4 00 04 06 10 00 81 00
Offset 010: 00 00 00 00 00 00 00 00 00 02 02 00 E0 E0 00 00
Offset 020: F0 FF 00 00 01 F0 01 F0 00 00 00 00 00 00 00 00
Offset 030: 00 00 00 00 40 00 00 00 00 00 00 00 03 02 04 00
Offset 040: 10 80 42 01 00 80 00 00 00 00 10 00 12 3C 12 02
Offset 050: 40 00 11 70 00 B2 0C 00 00 00 40 00 00 00 00 00
Offset 060: 00 00 00 00 16 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 0D A0 00 00 CF 10 58 17 00 00 00 00 00 00 00 00
Offset 0A0: 01 00 02 C8 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Navigation

Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 01 02 0B 00 00 00 80 11 01 00 00 00 00
Offset 0E0: 00 03 00 00 00 00 00 00 01 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1D F00: Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C1]

Offset 000: 86 80 26 1E 06 00 90 02 04 20 03 0C 00 00 00 00
Offset 010: 00 70 C1 F7 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 17 01 00 00
Offset 040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 58 C2 C9 00 00 00 00 0A 98 A0 20 00 00 00 00
Offset 060: 20 20 01 06 00 00 00 00 01 00 00 01 00 20 00 00
Offset 070: 00 00 FF 3F 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 80 00 11 88 0C 93 30 0D 00 24 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 13 00 06 03 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 AA FF 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 84 90 95 DA
Offset 0F0: 00 00 00 00 88 85 80 00 87 0F 05 08 08 17 5B 20

B00 D1E F00: Intel 82801xx I/O Controller Hub

Offset 000: 86 80 4E 24 07 00 10 00 A4 01 04 06 00 00 01 00
Offset 010: 00 00 00 00 00 00 00 00 00 03 03 20 F0 00 80 22
Offset 020: F0 FF 00 00 F1 FF 01 00 00 00 00 00 00 00 00 00
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 FF 00 04 00
Offset 040: 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 10
Offset 050: 0D 00 00 00 CF 10 58 17 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1F F00: Intel B75 Chipset - LPC Interface Controller [C1]

Offset 000: 86 80 49 1E 07 00 10 02 04 00 01 06 00 00 80 00
Offset 010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00 00
Offset 040: 01 04 00 00 80 00 00 00 01 05 00 00 10 00 00 00
Offset 050: F8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 8B 83 8A 8A 90 00 00 00 80 80 85 8B F8 F0 00 00
Offset 070: 78 F0 78 F0 78 F0 78 F0 78 F0 78 F0 78 F0 78 F0
Offset 080: 10 00 05 34 81 06 3C 00 00 00 00 00 81 06 FC 00
Offset 090: 01 47 0C 00 00 00 00 00 00 00 00 00 00 00 00 00

Navigation

Offset 0A0: 08 0A 80 00 49 3C 06 00 00 47 00 00 00 00 00 80
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 33 22 11 00 67 45 00 00 CF FF 00 00 08 00 00 00
Offset 0E0: 09 00 0C 10 00 00 00 00 19 06 E4 04 00 00 00 00
Offset 0F0: 01 C0 D1 FE 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1F F02: Intel Panther Point PCH - SATA AHCI Controller [C1]

Offset 000: 86 80 02 1E 07 04 B0 02 04 01 06 01 00 00 00 00
Offset 010: B1 F0 00 00 A1 F0 00 00 91 F0 00 00 81 F0 00 00
Offset 020: 61 F0 00 00 00 60 C1 F7 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 80 00 00 00 00 00 00 00 02 00 00
Offset 040: 00 80 00 80 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 01 A8 03 40 08 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 70 01 00 0C F0 E0 FE 50 49 00 00 00 00 00 00
Offset 090: 60 2E 11 91 83 01 00 2E 08 42 5C 01 00 00 00 00
Offset 0A0: E0 00 00 00 39 00 00 00 12 B0 10 00 48 00 00 00
Offset 0B0: 13 00 06 03 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1F F03: Intel Panther Point PCH - SMBus Controller [C1]

Offset 000: 86 80 22 1E 03 00 80 02 04 00 05 0C 00 00 00 00
Offset 010: 04 50 C1 F7 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 41 F0 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 00 00 00 00 00 00 00 00 0A 03 00 00
Offset 040: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 03 04 04 00 00 00 08 08 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B00 D1F F06: Intel Panther Point PCH - Thermal Management Controller [C1]

Offset 000: 86 80 24 1E 00 00 10 00 04 00 80 11 00 00 00 00
Offset 010: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 CF 10 58 17
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 0A 03 00 00
Offset 040: 05 00 A0 DF 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 00 23 00 08 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Navigation

Offset 080: 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 05 08 00 00 00 00

B02 D00 F00: Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter

Offset 000: EC 10 68 81 07 00 10 00 07 00 00 02 10 00 00 00
Offset 010: 01 E0 00 00 00 00 00 00 0C 40 00 F0 00 00 00 00
Offset 020: 0C 00 00 F0 00 00 00 00 00 00 00 00 CF 10 5A 17
Offset 030: 00 00 00 00 40 00 00 00 00 00 00 00 11 01 00 00
Offset 040: 01 50 C3 FF 08 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 05 70 80 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 10 B0 02 02 C0 8C 90 05 00 50 10 00 11 7C 07 00
Offset 080: 40 00 11 10 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 1F 00 00 00 10 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 11 D0 03 00 04 00 00 00 04 08 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 03 00 FC 80 FF FF FF FF 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0150: Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 4000: 66 66 14 00 44 43 10 86 00 00 00 00 6A 59 00 00
Offset 4010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00
Offset 4020: 05 00 10 00 20 20 20 20 00 00 0E 00 00 00 00 00

PCI-8086-0150: Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 4200: 02 00 06 00 00 04 06 00 00 00 00 00 00 00 00 00
Offset 4210: 00 00 00 00 88 02 00 00 00 00 00 00 00 00 00 00
Offset 4220: 07 00 00 00 03 F0 01 00 00 00 00 00 00 00 00 00
Offset 4230: 01 10 0F 00 01 10 90 01 00 00 00 00 00 00 00 00
Offset 4240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4280: 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00
Offset 4290: 80 40 00 00 0F 98 00 00 04 10 B4 46 00 00 00 00
Offset 42A0: 00 00 00 00 00 B2 00 01 00 00 00 00 00 00 00 00

PCI-8086-0150: Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 4400: BB 8B 1C 00 65 64 18 0C 20 42 04 0A B4 58 00 00
Offset 4410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00
Offset 4420: 05 00 10 00 29 20 20 20 03 00 0E 00 00 00 00 00

PCI-8086-0150: Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

```
Offset 4600:    00 00 46 00 20 03 00 00 20 03 00 00 00 04 06 00
Offset 4610:    44 02 00 00 42 02 00 00 42 02 00 00 40 02 00 00
Offset 4620:    06 F0 01 00 01 F2 01 00 05 F1 01 00 02 F0 01 00
Offset 4630:    04 20 28 00 64 10 28 08 64 10 28 04 01 0C 28 00
Offset 4640:    00 00 00 00 E3 07 04 00 E3 07 04 00 00 00 00 00
Offset 4650:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4660:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4670:    47 9F B0 A9 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4680:    00 00 00 00 00 00 0C 00 00 00 00 00 44 00 00 00
Offset 4690:    80 40 00 00 FF 98 00 00 60 18 D0 6C 18 02 00 00
Offset 46A0:    01 10 00 00 00 82 F8 41 00 00 00 00 01 00 00 00

PCI-8086-0150:  Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 4800:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4810:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0150:  Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 4A80:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4A90:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0150:  Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 5000:    21 00 00 00 00 00 60 00 10 00 60 00 00 00 60 00
Offset 5010:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0150:  Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 5880:    E7 71 91 CA 00 00 00 00 D0 DA E4 00 00 00 00 00
Offset 5890:    00 00 00 00 B0 A9 14 03 00 00 00 00 00 00 00 00
Offset 58A0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58B0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58C0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58D0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58E0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58F0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 5900:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 5910:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 5920:    00 00 00 00 18 00 00 00 A6 0F D3 2B B1 07 E9 00
Offset 5930:    B8 01 60 01 00 00 0D 00 03 10 0A 00 66 D6 A2 3D
Offset 5940:    FB 0B 2C 13 A9 BE 58 0A 00 07 00 00 00 00 00 00
Offset 5950:    00 00 00 00 00 00 04 00 00 21 01 E0 00 10 08 00
Offset 5960:    B0 41 1C 7E 4F AA 3E CE 14 A2 3E CE 9F 59 5D 3A
Offset 5970:    D0 F1 DB 7B D0 F1 DB 7B 37 00 00 00 37 00 00 00
Offset 5980:    37 00 00 00 80 B8 F1 55 00 00 00 00 00 00 00 00
Offset 5990:    FF 00 00 00 FF 00 00 00 15 0D 07 00 00 14 69 00
Offset 59A0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 59B0:    80 03 00 80 94 14 14 18 70 01 00 80 94 14 14 18
Offset 59C0:    00 00 32 88 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0150:  Intel SNB/IVB/HSW/CRW/BDW/SKL/KBL/CFL/WHL/CNL/CML/ICL/RKL/TGL MCHBAR

Offset 5E00:    06 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00
```

Navigation

```
Offset 5E10:      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-1E24:    Intel 5/6/7-series PCH TBAR

Offset 00:        01 BA 00 DD 2B 3A 00 00 84 04 04 00 00 00 C0 00
Offset 10:        00 00 40 1A 87 DE 8C 80 00 00 00 00 00 00 00 00
Offset 20:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 30:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
Offset 40:        01 02 00 FF 00 00 00 00 00 00 00 00 00 00 00 00
Offset 50:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 60:        00 00 00 00 00 00 00 00 00 00 00 00 20 1B 16 05
Offset 70:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 80:        01 01 00 04 5E 5E 00 FF 00 00 00 00 00 00 00 00
Offset 90:        16 AA DF 18 00 00 00 00 00 00 00 00 00 00 00 00
Offset A0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset B0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset C0:        01 01 00 00 00 00 FF 00 00 00 00 00 00 00 00 00
Offset D0:        00 00 00 00 00 00 00 00 00 00 00 00
```

Debug - Video BIOS

```
C000:0000   U.r...000000000000.#.-"U@...00IBM VGA Compatible BIOS. .t.......
C000:0040   PCIR.............................."...R.Z.b.j.r.....t.............
C000:0080   .................=.............................................DH.
C000:00C0   ....DH.....DH....0DH.....DI.....DI.....DJ.....DJ....0DJ.....DI..
C000:0100   ..0DI.....DJ.....DK.....DK.....DK....0.L......L......L....0.L...
C000:0140   ...M......M.....0.J..2.n..4....8....:....<....A.J..C.n..E....I..
C000:0180   ..K....M....P J..R n..T ...X ...Z ...\ ...` .5..a.5..b 5..c.O..d.
C000:01C0   O..e O..f.i..g.i..h i..i....j....k ...l....m....n ...o....p....q
C000:0200   ...}....~....  ........ .-..` ............. .1..l...........rQ..
C000:0240   n(U...!....... ....`"........... ....@.......... .1X. (.........
C000:0280   V. .1X. .P........d..@A.&0..6.......... A. 0.`........0*..Q.*@0p
C000:02C0   .........4..Q.*@..........H?@0b.2@@.........h[..r.<P............
C000:0300   ........E.............................................E..........
C000:0340   ........................For Evaluation Use Only....(........c-'
C000:0380   (.+.....................................................(........c-'
C000:03C0   (.+.....................................................P........c_O
```

Debug - Unknown

```
Motherboard   63-0100-000001-00101111-122211-Chipset$JIB75Y3409_
Motherboard   DMIMOBO: FUJITSU JIB75Y3
Motherboard   DMISYS: FUJITSU FMVD0400D
Motherboard   Unknown
SSD           P3-128
```

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.